

Identity Theft: A Study in Contact Centres

Iain Moir¹, George R. S. Weir²

¹Department of Management, University of Strathclyde,
Glasgow G4 0QU, UK

²Department of Computer and Information Sciences, University of Strathclyde,
Glasgow G1 1XH, UK
iain.moir@strath.ac.uk, george.weir@cis.strath.ac.uk

Abstract. This paper explores the recent phenomenon of identity theft. In particular, it examines the contact centre environment as a mechanism for this to occur. Through a survey that was conducted amongst forty-five contact centre workers in the Glasgow area we determined that contact centres can and do provide a mechanism for identity theft. Specifically, we found a particularly high incidence of agents who had previously dealt with phone calls that they considered suspicious. Furthermore, there are agents within such environments who have previously been offered money in exchange for customers' details, or who know of fellow workers who received such offers. Lastly, we identify specific practices within contact centres that may contribute to the likelihood of identity theft.

Key words. Identity Theft, Identity Fraud, Contact Centre, Call Centre

1. Introduction

In recent years the phenomenon of identity theft has gained wide spread media coverage and has grown to be a concern for individuals and businesses alike [1, 2]. Of particular note are exploits which may occur within contact centres [3]. In such environments it is possible for a fraudster to bribe contact centre agents for customer's personal details. Identity fraudsters may themselves gain employment in contact centres in order to gather such information directly. Lastly, culprits may try to coerce an agent into releasing information over the phone by means of social engineering. Unfortunately, many contact centre agents are unaware of such risks and are untrained in how to deal with them. This can result in severe financial loss to the customer along with the associated psychological trauma from having their identity stolen.

In this paper we explore the nature of identity theft in a contact centre context and investigate the associated problems that can arise from this. In addition, we criticise practices within contact centres that may facilitate such exploits.

-
- Presented at the 4th International Conference on Global E-Security, University of East London, June 2008.

1.1 Definition

For the purposes of this paper, we will apply the Home Office definitions of identity theft and identity fraud [4]:

***Identity Theft** – Occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual the victim is alive or dead.*

***Identity Fraud** – Occurs when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation / liability by falsely claiming that he / she was the victim of identity fraud. Examples include: using a false identity or someone else's identity details (name, address, date of birth etc) for commercial or monetary gain, to obtain goods or access facilities or services e.g. opening a bank account, applying for a loan or credit card.*

There is a clear distinction between two related but separate acts – identity theft and identity fraud. Under the Fraud Bill (2006) the act of identity fraud would be the actual crime committed, while identity theft would be a precursor to that crime. This account also gives example contexts for identity fraud, for example opening a bank account or applying for a loan or credit card. This indicates that there is also a distinction between identity fraud and other exploits such as credit card fraud. In credit card fraud the fraudster would use the victim's credit card details to access the victim's account directly. This is not considered identity theft since the fraudster did not use this information to apply for credit in the victim's name.

In the United States a much broader definition is given under the Identity Theft and Assumption Deterrence Act 1998 (ITADA). Under this Act, offences which may have previously been classed as credit card fraud are now considered identity theft [5]. This include schemes such as creating counterfeit cards, stealing credit cards (either from the person or from mail containing cards in transit) and would also include card-not-present purchases over the internet. This broader account may contribute to identity theft being dubbed the fastest growing white-collar crime in the United States [6]. Although other varieties of identity theft may be characterised [7, 8], for present purposes we only consider identity theft as a means to financial gain.

1.2 Mechanisms

In a study by Duffin et al [9], five people who had previously committed identity theft were interviewed. One offender in the study stated, '*All you are stealing is the credit worthiness to get the most money you can from it.*' If credit worthiness is the primary goal of an identity thief then it appears that those at greatest risk of being victims are those who are financially well off. Simple techniques for obtaining personal information were stealing handbags or wallets, snatching mail from doormats and obtaining documents as a result of a burglary or car theft. More sophisticated methods involved

obtaining information from the electoral role or buying details from individuals with access to personal information. One highlighted scheme had the fraudster paying an estate agent friend to lease him vacant properties, which could later be used to receive redirected victim's mail. Typically, the fraudster would phone the victim's utility company with a change of address enquiry. Once the redirected utility bills were in hand they could be used as proof of identification.

Surprisingly, 'bin raiding', a strategy often cited in the media, as a primary means of identity theft, is probably the least likely mechanism for obtaining information. One offender commented, '*Rummaging through bins – with regards to that ...don't think this happens. The thought of loads of people trawling through bins is not true; there are easier ways of getting it.*' Similar views were expressed by other offenders.

One particularly effective mechanism is Social Engineering. Here, a fraudster phones up the victim pretending to be someone else in order to retrieve confidential information. An example of this would be someone phoning up a bank official pretending to be from the IT department to retrieve passwords or customer information for misuse. Mitnick [10] explains that Social Engineering is often effective because many company security systems fail to accommodate the 'human factor'. Other studies show that individuals with little or no training can become efficient social engineers [11].

1.3 Identity Theft within Contact Centres

The main context examined in this paper is the intersection of fraudsters and contact centres. This may involve fraudsters offering money to agents in exchange for personal details, fraudsters gaining employment to access details directly or fraudsters using social engineering over the phone to trick agents into releasing details. Before reviewing this further, let us consider how such exploits would fit into a fraudster's scheme for financial gain.

One reason why fraudsters target contact centre workers could be the conflicting demands placed upon such employees. Fleischer [12] shows that, on the one hand, agents are expected to be helpful and polite; whilst, on the other, they must be wary and restrained if they can not be sure with whom they are dealing. In addition to this, there is the prospect that by asking too many questions agents may offend the customer and lose business. If the insult rate is too high, the consumer will go somewhere else or will use a different medium to complete the transaction [13]. So there is a fine balance to be struck between being helpful, ensuring the safety of information and not enquiring too much into a customer's details.

Another reason why contact centres are targeted is that the identification process used is not as strong as would be the case if a customer made an enquiry in person. Clarke [14] defines human identification as '*...the association of data with a particular human being.*' In the case of contact centres a *knowledge-based* system of identification is used where an individual is in possession of knowledge that only that person would be expected to know. For example, a Personal Identification Number (PIN) or a password. Problems may arise with this system of identification where a password is not present on the account or the password is common and easy to guess. Because the identification is undertaken over the phone no other system of identifica-

tion, such as *token-based*, passport or driving license, is available. Therefore, the identification method along with pressures to be helpful and understanding to the customer, may contribute to contact centres being targeted by fraudsters.

2. Research method

A survey of contact centre workers within the Glasgow area was conducted. Participants were asked to complete a self-administered structured questionnaire with a total of thirty-nine list (yes/no) questions. A snowball sample was employed - initial contact was made with several agents and this led to further introductions and more data collection. Due to the closed nature of the questionnaire more in-depth information was gathered through a series of interviews with selected respondents.

Data was gathered from a total of forty-five respondents. Each respondent had access to customer's personal details and 87% had access to sensitive details such as bank or credit card data. The majority of respondents worked with inbound calls and 80% were either students in higher education or had been students in the recent past. Through leads which arose during the data collection, it was possible to survey three major contact centres and the questionnaire was completed by ten workers in each organisation. Each of these organisations represented a different industry sector - one was a large branded financial institution, another was a large branded telecommunications firm and the other was a third-party call handler. In the following, these organisations will be referred to as *Finance*, *Telecom* and *Outsource* respectively. A worker from another large financial organisation was interviewed and is referred to as *Finance2*. During this research consideration was given to ethical issues and the requirement for participants' anonymity.

3. Results

3.1 The Market for Customer's Details

The questionnaire indicated that 73% of workers had dealt with a call they considered suspicious. In all but one case this was reported to management. In *Finance*, 100% reported that they had dealt with a suspicious phone call. This supports the view that the financial services sector bears the brunt of attacks involving fraud. In *Telecom* and *Outsource*, 60% and 70% of workers felt that they had dealt with suspicious phone calls respectively.

Of the individuals who completed the questionnaire, 22% said they had worked with people whom they considered suspicious. Only two people in *Finance* had felt this way, whereas in *Telecom* four people felt like this and in *Outsource* there were three. A possible reason why this number was less within *Finance* is that financial institutions are more likely to check employee references as a security measure.

Of course, suspicions do not directly equate to guilt. Further questions were asked to reveal more information on the extent of contact centre workers involvement in this type of exploit. One of the survey questions asked, 'have you ever been offered money in exchange for other people's details.' One person answered yes – in percentage terms this accounted for 2% of the total sample. A further question was asked, 'do you know of anyone who has previously taken money in exchange for other people's details?' Two people answered positively, accounting for 4% of the total sample. The two people who answered yes to this question worked in different contact centres with no common link so there is very little chance that they would be accounting for the same person.

From these results we may conclude that there is a definite market for people's details within the Glasgow area and that contact centres do afford a context for this to occur. Although the results may not be representative they serve as a useful indicator. Whether the agent who was offered money in exchange for other people's details actually accepted such an arrangement was not asked.

3.2 Security Practices within Contact Centres

If it has then been established that contact centres can and do provide a mechanism for identity theft to occur then the next logical question would be, what security measures are in place within contact centres that would prevent such an exploit from happening? What follows are security issues within contact centres that are deemed to be of a severe nature. These are issues that were raised both in the questionnaire and in the follow up interviews.

3.21 Training

Training within the three main contact centres surveyed varied widely. *Finance* received the most training at six weeks full time. However, only a few hours were dedicated to security issues. *Finance2* received two weeks training and received a presentation from the head of the Fraud Department in which scenarios were played out on how a possible fraudster could access sensitive information. *Outsource* again received two weeks training however only one hour was spent on security issues and very little emphasis was given to the Data Protection Act.

In all of the main contact centres there was no further structured training available on security either by request or by regular mandatory updates. In the financial firms both interviewees stated that if they had any issues they were encouraged to speak to their team leader. In *Outsource* additional ad hoc training was available to those members of staff who were identified as needing help – in this case security was seen as an inherent part of call quality. In all of the interviews that were conducted each respondent expressed concerns over the level of training.

3.22 Customer Identification

It was stated in a previous section that the identification system that contact centres use in order to confirm a customer's identity was that of a *knowledge-based* system where the individual would remember a password or personal identification number

in order to confirm their identity. However, in one of the contact centres, *Finance2*, customers did not need nor were encouraged to put a password onto their account. Instead security questions were asked such as name, address, account number and date of birth. This information would not fulfil the criteria set out in a *knowledge-based* system as such information could be easily known by other individuals.

Of course there will be occasions where the customer may have forgotten their password and security questions will have to be asked. In order to make a successful identification the questions would need to be of significant complexity that it would be difficult for a fraudster to access sensitive information. This would exclude such obvious information such as the customer's mother's maiden name which can easily be accessed by a knowledgeable fraudster. Despite this agents within *Telecom* do ask for the customer's mother's maiden name as part of their security protocols. A more secure identification method was found in *Outsource* where a list of suitable questions was provided to agents in order that possible fraudsters have a reduced chance of getting access to sensitive information.

What is perhaps of some concern is that 11% respondents said that they had at some point allowed a customer access to their account without first asking them any security questions - whether this happened on more than one occasion from each respondent remains to be seen. A worker at *Finance* had this to say about this statistic,

Oh it's higher than that – definitely. It sounds really daft but sometimes you forget to ask the security questions... everybody's done it; it's human nature to forget these things.

The interviewee went on to say that she had previously worked in a contact centre where the computer system would ask for certain letters of the password and would not allow the worker to progress with the phone call until this condition was met. Obviously, this system will not have been in place for all of the agents who responded to this questionnaire or the response rate for this question would be zero. What can be said is that where a computer system is not in place to prompt the user and human nature is relied upon to ask for security information there will be a degree of non-conformance by agents.

3.23 Computer Policy

With regard to computer procedures, questionnaire respondents confirmed that each had a unique login ID, 91% were not allowed to download applications from the Internet and 96% were regularly prompted to change their password. However, only 36% were using login time-outs, only 67% were required to employ passwords with a mixture of alphabetic and numeric characters and 67% said that they had access to email at work. This would allow access to another's terminal should they forget to log out. Once logged into the company's network a dictionary attack could be carried out to identify common passwords for other user accounts. In addition, access to email at work affords scope for employees to send customer account information to external recipients. Of key importance with regard to computer policy is the way in which people react to procedures set down by the company. If policy is not enforced then an 'easy going' culture develops where the policy principles are not taken seriously. As an example, a worker at *Outsource* stated,

...I see quite regularly someone who has become locked out of the system and one of the managers will give them another ID to use; sometimes the ID of an agent who has just left or the ID of someone else who is on the floor but is not using it.

Such loose behaviour leaves an inaccurate audit trail and may render the source of any security breach difficult to trace back to the true perpetrator. By the time it is traced, the fraudster could have moved on and may only have committed dubious acts whilst using a colleagues login details. This issue could be particularly problematic where there is a high turnover of staff. A survey of staff turnover rates by the Call Centre Association [15] indicates that over 50% of call centres have a turnover rate for permanent, full time staff of over 10% per annum. This context underlines the need for vigilant enforcement of computer policies in contact centres.

3.24 Pen & Paper

Surprisingly, 100% of questionnaire respondents were allowed to take pen and paper onto the contact centre floor. *Finance* appeared strictest on this issue where workers were provided with pen and paper by the company, which then had to be placed in a locker at the end of the day. *Outsource* did not have lockers, but provided shredders for disposal of all scrap containing sensitive information. *Outsource* also employed random bag searches as part of its security measures. However, this was more focused on detection of mobile phones.

The semi-structured interviews asked if there were obstacles in place to stop an individual from noting customers' details using pen and paper and walking home with that information. In every case, interviewees indicated that there was nothing to stop this from happening - even when lockers were placed onsite. An incident is detailed below that reflects the risks of allowing pen and paper onto the contact centre floor.

...there were two people (I didn't know them) that actually got escorted out of the premises. There were undercover police working in different departments monitoring them and their behaviour. They found them taking people's details using newspapers at their desk and they were writing the account numbers in the crossword puzzles. The police were called in and they were handcuffed and frog marched out.

Of course, some contact centre workers will need pen and paper for their daily duties. Such workers should be clearly identified, provided with pen and paper along with a locker to store such items and random bag searches should take place to ensure that data is not removed from the premises.

3.25 Mobile Phones

Mobile phones represent a similar hazard to security, especially where the phone has a camera that could be used to take a photograph of account details. Our interviews showed that each company had a different policy in this regard. In *Finance* mobile

phones were meant to be stored in lockers along with any pens and paper that workers may have in their possession. Within *Finance2*, the policy required that workers were not seen using mobiles, and in *Outsource*, mobile phones were permitted onto the floor but a strict policy required that they were switched off; regular bag searches were conducted to ensure this and any worker caught with a mobile phone switched on would be subject to disciplinary action. Despite such measures there was an occasion where a worker completely breached this protocol:

I actually saw one of the younger members of the team... taking a photograph of a customers' account details on his mobile phone. The customer's name looked humorous and because of that he said he wanted to take a photograph and show it to his mates. I pointed out to him not only did that screen have the customers name on it, it had basically every piece of information that you would need in order to access someone's account. I told him to get it off his phone.

On this occasion the motivation was not to commit identity theft, merely an attempt to have a cheap joke at someone else's expense. But the example illustrates the dangers of allowing mobile phones onto the contact centre floor. Curiously, the third party call handler had the most stringent procedure in place with regards to mobile phones. The other two companies, both large financial companies, were less strict in mobile phone control. *Outsource* not only had strict mobile management procedures, but these were enforced at many different levels. For example, random bag searches were used to monitor the situation and disciplinary action was enforced against any employee breaching company policy. These actions develop a culture within the organisation that mobile phones are not allowed to be switched on whilst on the contact centre floor. As illustrated by the previous example, this culture ensures that an employee who witnesses such an act treats the matter seriously. The milder attitudes at the other two financial companies leave them vulnerable to such security breaches.

4. Conclusions

Contact centres can provide a rich setting for identity theft. Our survey indicated a high incidence of contact centre workers who had dealt with a phone call they thought was suspicious. From our survey of forty-five contact centre workers, one had previously been offered money for customer's details and a further two knew of others who had previously been offered money. Of course we expect some degree of reticence when people are asked such questions, so the true extent of incidents where fraudsters offer money to workers for customer's details will remain difficult to measure. Nevertheless, evidence indicates a serious threat to data privacy within contact centres.

References

1. Economist. *What's in a Name? Identity Theft*. Economist (U.S. Edition). 3rd March, 2005.
2. Guardian. *What could a boarding pass tell an identity fraudster about you? A. Way too much*, 2006. Available from: <http://www.guardian.co.uk/idcards/story/0,,1766266,00.html> [Accessed 21st March 2008]
3. Stockford, P. *A Banner Year for Identity Theft*. Call Centre Magazine, Vol. 19, No. 12, pp 16, 2006.
4. Home Office. *Identity Crime Definitions*, 2006. Available from: <http://www.identity-theft.org.uk/definition.html> [Accessed 21st March 2008].
5. Binder, R., & Gill, M. *Identity Theft & Fraud: Learning from the U.S.A.* Leicester. Perpetuity Research & Consultancy International Ltd, 2005.
6. Economist. *Stealing People is Wrong*. Economist (U.S. Edition). March, 2001.
7. Perl, M. *It's not Always About the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft*. Journal of Criminal Law & Criminology, Vol. 94 No. 1, pp 169-208, 2003.
8. Ramaswamy, V. M. *Identity-Theft Toolkit*. CPA Journal, Vol. 76, No. 10, pp 66-70, 2006.
9. Duffin, M., et al. *Identity Theft in the UK: Offender and Victim Perspective*. Leicester. Perpetuity Research & Consultancy International Ltd, 2006.
10. Mitnik, K. *The Art of Deception*. Wiley Publishing: Indiana, 2002.
11. Endicott-Popovski, B. & Lockwood, D. L. *A Social Engineering Project in a Computer Security Course*. Academy of Information & Management Sciences Journal, Vol. 9, No. 1, pp 37 – 44, 2006.
12. Fleischer, J. *An Ounce of Prevention*. Call Centre Magazine, Vol. 18, No. 11, pp 56, 2005.
13. Willcox, N. A., & Regan, T. M. *Identity Fraud: Providing a Solution*. Journal of Economic Crime Management, Vol. 1, No. 1, 2002.
14. Clarke, R. *Human Identification in Information Systems: Management Challenges & Public Policy Issues*. Information Technology & People, Vol. 7, No. 4, pp 6 – 37, 1994.
15. CCA. *Counting the True Cost of Staff Turnover*, 2001. Available from: <http://www.cca.org.uk/documents/Blue%20Sky%20Counting%20the%20True%20Cost%20of%20Staff%20Turnover%20Report.pdf> [Accessed 21st March 2008],