15

Fraud and its PREY: Conceptualising Social Engineering Tactics and its Impact on Financial Literacy Outcomes

Jacqueline M. Drew
is a Lecturer in the School of Criminology and Criminal Justice at Griffith University and an Associate Investigator with the Australian Research Council (ARC) Centre of Excellence in Policing and Security (CEPS). She has worked as a practitioner and researcher across a number of police agencies. Her research interests include white collar crime (particularly, financial fraud); recruitment, retention, leadership and performance management within policing; and organisational structure and systems relating to innovative police practice. She has written on topics including Ponzi schemes, fraud curriculum, carbon fraud, third-party partnerships and human resource management in policing.

Cassandra Cross
is a Lecturer in the School of Justice, Faculty of Law, Queensland University of Technology (QUT). Before this, she worked as a research and senior policy officer within the Queensland Police Service, where she worked across a number of portfolios, most notably online fraud. Her research focused specifically on seniors' online fraud experiences, which has generated both national and international interest. In 2011, she was awarded the Donald Mackay Churchill Fellowship for Organised Crime, which enabled her to travel to the United Kingdom, United States and Canada to examine other jurisdictional responses to online fraud prevention and victimisation.

Introduction

An unexpected finding within the financial literacy debate centres on the relationship between financial literacy levels and fraud victimisation. It has often been assumed that increasing financial literacy levels would also act as a protective factor for individuals falling victim to

Journal of Financial Services Marketing, 18, 188–198, 2013, DOI:10.1057/fsm.2013.14. 'Fraud and its PREY: Conceptualising social engineering tactics and its impact on financial literacy outcomes', by Jacqueline M. Drew and Cassandra Cross.

financial and investment fraud. While some support for this assumption has been found (for example, Gamble *et al*, 2012; Lusardi, 2012), a number of researchers have in fact reported that financial literacy is associated with higher levels of victimisation (NASD, 2006; American Association of Retired Persons (AARP), 2007, 2008, 2011; Australian Crime Commission (ACC) and Australian Institute of Criminology (AIC), 2012). The NASD Investor Education Foundation (now FINRA Investor Education Foundation), concluded that 'financial literacy programs are necessary but probably not sufficient to prevent fraud' (NASD, 2006, p. 6). This represents a major challenge for the financial literacy agenda.

This article makes a positive contribution to the financial literacy field through its examination of an approach that not only strives to more effectively address the challenge of financial fraud but can also be used as a proactive, fraud prevention framework. This article uses investment fraud, which involves the selling of (usually) fraudulent investment products at inflated prices (also referred to as boiler room fraud) as an illustrative case study. The article explores how victimisation could be better understood through analysing the application of social engineering theory and persuasion tactics used by offenders in perpetrating fraudulent investment schemes. The PREY (Profiled, Relational, Exploitable, and Yielding) model, developed in this article based on a review of the literature, captures and summarises those psychological tactics used by fraud perpetrators to influence the thoughts and decision-making processes of individuals. Relevant to financial fraud, the model seeks to move financial literacy education towards an expanded curriculum, going beyond knowledge and application of financial matters and generic warnings about financial fraud. It is concluded that the curriculum needs to explicitly include education on social engineering and persuasion techniques. This approach is likely to be relevant across all offerings of financial literacy education. However, education focused on social engineering and persuasion techniques may be more relevant to groups with particular characteristics. For example, as will be discussed later in this article, research has demonstrated a strong correlation between age, levels of financial literacy knowledge and investment fraud victimisation (NASD, 2006; AARP, 2011).

Definition and prevalence of investment fraud

To begin, it is important to define investment fraud and to consider its prevalence. Prevalence rates of investment fraud provide some basis on which to assess the need and urgency for fraud education to be prioritised within the financial literacy curriculum.

Investment fraud through the use of cold calling (or boiler room fraud) can be seen to operate through four distinct phases. While these may be unique to individual situations, there is a general pattern that can be characterised by the stages below:

(1) Initial approach by the offender to the potential investor, outlining the opportunity and seeking approval to send documentation about the potential investment.
(2) Follow up by the offender to confirm the receipt of the marketing materials and solicit a financial commitment to the investment opportunity.
(3) Continued contact by the offender to reassure the victim of their investment, and to offer additional investment opportunities.
(4) A crisis point, where the victim (for whatever reason) wants to exit their investment but is informed that they cannot do this. The victim may then be convinced to reinvest in another opportunity or alternatively may begin to suspect that they have been defrauded.

Turning to the issue of prevalence, investment fraud represents a significant threat to financial security. In 2011, the ACC established Taskforce Galilee to examine the issue of serious and organised investment fraud in Australia. This taskforce estimated that between January 2007 and April 2012 more than A$113 million was lost by over 2600 victims (ACC and AIC, 2012). Serious and organised investment fraud was defined as:

(a) Any unsolicited contact, by telephone or Internet, of persons in Australia (potential investors) by persons (callers) usually located overseas, where such callers engage in conduct that is fraudulent, false, misleading or deceptive with the purpose of inducing potential investors to buy, sell or retain securities or other investments and where such callers do not have the licence or authority to engage in a securities business, or investment advice business in Australia; and
(b) May include superannuation and investment fraud' (ACC and AIC, 2012, p. 5).

Earlier research by the Australian Securities and Investment Commission (ASIC), reported that between 1999 and 2002 more than 7300 people across Australia had contacted them in relation to a cold calling experience (ASIC, 2002a). Approximately, 80 per cent of these people had lost money (ASIC, 2002a). At this time, ASIC conservatively estimated that victims may have been defrauded in excess of A$400 million (ASIC, 2002a).

These Australian findings are echoed across the United Kingdom and the United States. In the United Kingdom, it is estimated that 3.5 billion pounds each year is lost by victims of mass marketing fraud (which includes investment fraud) (National Fraud Authority (NFA), 2012), and in the United States the comparable annual fraud cost has been calculated to be in excess of $50 billion (Deevy *et al*, 2012).

Given the prevalence of fraud and the generally accepted assumption that these statistics are likely to grossly underestimate its true impact, this type of fraud has serious implications for the financial well-being of those victimised. In this article, financial well-being is defined as 'a state of being financially healthy, happy, and free from worry' (Joo, 2008, cited in Malone *et al*, 2010, p. 63). Financial literacy certainly has a role to play in working towards minimising and preventing investors being defrauded. However, as the following discussion will explore, the answer does not necessarily lie with simply increasing financial literacy levels. The relationship between financial literacy and fraud prevention is more complex.

Relationship between financial literacy and fraud outcomes

As discussed earlier, financial literacy may not be as effective as previously thought in protecting against fraud victimisation. The ACC and AIC's (2012) report on the outcomes of Taskforce Galilee found that victims of investment fraud were more financially literate, had previously invested in other companies and appeared on shareholder registers. Research conducted with older persons has been particularly consistent in this finding. Research conducted by NASD (2006) found that older victims of financial fraud compared with non-victims actually scored higher on tests of financial literacy knowledge. This was similar to conclusions drawn in earlier research published by the AARP (2007, 2008, 2011).

The financial literacy and fraud victimisation relationship creates a significant challenge to those involved in financial literacy as an often-stated goal of financial literacy involves fraud education (Taskforce on Financial Literacy, 2010). A rudimentary analysis of the research could lead to the conclusion that financial literacy education, particularly in respect to fraud victimisation, is simply counterproductive. As a specific example, the argument is logical when reflecting on data that suggests that higher rates of financial literacy is generally correlated with age (ANZ, 2011), and in turn age is often correlated with higher levels of

financial fraud victimisation (NASD, 2006; AARP, 2011). However, the implication of this research is not of course to discontinue efforts to improve financial literacy levels. What is needed is a reexamination and deeper consideration of the relationship between financial literacy, fraud, current approaches used in the financial literacy curriculum and identifying and focusing education efforts on those most at risk of victimisation. The essential issue is how the financial literacy curriculum can be improved to address and ultimately prevent this spurious outcome.

A large research study conducted by NASD (2006) provides some useful insights into why financial literacy may be correlated with higher levels of victimisation. In turn, the research allows important conclusions to be drawn in respect to how the financial literacy curriculum could be redesigned in order to more effectively tackle financial fraud.

The NASD (2006) report, in seeking to account for their findings correlating financial literacy with increased victimisation rates, proposes three possible explanations. The researchers propose that one reason that those who are more financial literate are vulnerable to fraud is that even though they theoretically know how to avoid fraud they fail to apply fraud protection and avoidance measures to their own situation. This is called the 'knowing-doing gap' (NASD, 2006). A further explanation is the 'expert snare' whereby individuals who are more financially literate have an overconfidence in their investment abilities and decisions (NASD, 2006). Other researchers have also discussed the overconfidence trap (Gamble *et al*, 2012). It has been calculated that 'one standard deviation increase in overconfidence in financial knowledge increases the odds of falling victim to fraud by 38 per cent' (Gamble *et al*, 2012, p. 3). Although these two explanations are useful, they provide less direction as to how the financial literacy curriculum could be redesigned to more effectively minimise fraud victimisation. It is argued in this article that the third explanation provided by NASD (2006), 'low persuasion literacy' is the key to redesigning the financial literacy curriculum. It has the potential to address the 'expert snare' and make inroads into the 'knowing-doing gap'.

NASD (2006) state that 'low persuasion literacy' exposes investors to fraud, despite their comparatively higher levels of financial literacy, because financial literacy does not inoculate investors from the psychological persuasion tactics used by fraud perpetrators. The effectiveness of financial literacy as it is related to financial fraud may be much more about awareness of fraud tactics than about financial knowledge. Although both are important, it is persuasion tactics that have perhaps

been the least directly acknowledged and addressed in the financial literacy curriculum.

On the basis of this premise, the following discussion begins by illustrating how victimisation can be understood through applying social engineering theory and the use of persuasion tactics by offenders in perpetrating fraudulent investment schemes. This analysis leads to the formulation of the PREY model. The PREY model is examined in the light of its proposed contribution to financial literacy education through its direct articulation of social persuasion and social engineering tactics, moving financial literacy curriculum beyond generic warnings about financial fraud. This article is focused on improving the content base and curricula of financial literacy education. The following discussion presents the key crime prevention messages that derive from this approach. In turn, the discussion highlights the target groups and types of educational contexts that would most benefit from this addition to financial literacy educational content.

Introduction to persuasion tactics and social engineering

The key tenets of social engineering have been built from an understanding of the psychology of persuasion tactics primarily from the social psychology literature (Rusch, 1999). While there are a number of definitions of social engineering, perhaps the most fundamental is that provided by Manske (2000). Manske (2000, p. 53) defines social engineering as 'the practice of acquiring information through technical and non-technical means'. Some definitions focus on the ways in which social engineers seek to gain unauthorised access to corporate computer systems and networks (Abraham and Chengular-Smith, 2010), or deceive people into sharing sensitive information (Power and Forte, 2006). Consistent across most definitions is reference to the primary goal of social engineering, being the capture of information or 'the use of trickery, persuasion, impersonation, emotional manipulation and abuse of trust to gain information or computer access through the human interface' (Thompson, 2006, p. 222).

The process of social engineering as discussed in this article draws on the key elements of social engineering as defined by Thompson (2006) to explain how offenders perpetrate investment fraud. However, in this article, the social engineering process defines the end goal of social engineering not just as personal information or the ability to gain computer/account access (although these may be an important part of the whole

victimisation experience), rather the end goal involves directly obtaining money or financial rewards from the victim. In other words, social engineering is a general act of deception. Similarly, Beaver (2009, p. 35) concludes 'social engineering is nothing more than exploiting human being for malicious purposes', and as such can easily be understood in terms of illegitimate financial gain.

The PREY model

Given the foundational premise of this article, that is, financial literacy education needs to be expanded to include a focus on techniques of social engineering and persuasion, the PREY model is presented. The PREY model is an acronym for: Profiled, Relational, Exploitable and Yielding. It has been formulated to articulate the skills and techniques used by offenders in perpetrating investment (boiler room) fraud and can be used to assist investors to better identify and protect themselves against such approaches. The PREY model challenges investors to cast themselves in a predator versus prey scenario. The actors are investors who are viewed as potential 'prey' and fraud offenders who are the 'predators'. The concept of PREY is able to illustrate the nature of interaction between the offender and potential investor, where the ultimate goal of an offender perpetrating boiler room fraud is to obtain money from victims, and they will do whatever is necessary to achieve the highest amount of financial gain possible.

The PREY model is graphically represented in Figure 15.1 to capture the stages in the cycle of victimisation. The outer arrows feeding into the PREY model articulate the social engineering phases, as defined by Mitnick and Simon (2002), which are relevant to each stage of the PREY model.

Profiled

Investors need to be aware that offenders will typically profile them before any contact. This correlates with the first phase of social engineering, the research phase (Mitnick and Simon, 2002; Bakhshi *et al*, 2009). In the profiled stage, the offender attempts to identify the weaknesses and vulnerabilities of a potential target before initiating the first phone call. Specifically, in the case of boiler room fraud, offenders garner details of potential investors or victims from a number of legitimate and illegitimate sources. Although there may be a number of methods by which the offender obtains information about the potential victim, the crucial step relates to what the offender does with that information.

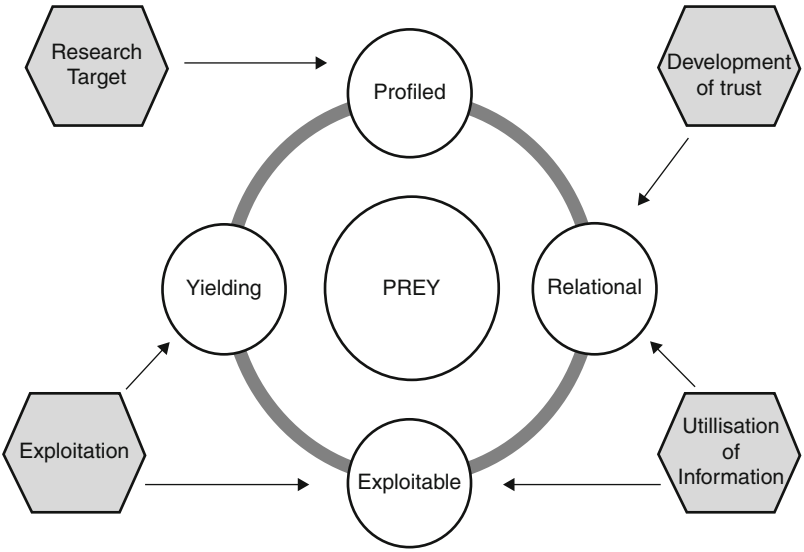

Figure 15.1 PREY framework

The offender is likely to already know key characteristics about the potential investor, including demographics, occupation and previous investment history (Workman, 2007a). This information is then used to specifically pitch the fraudulent investment opportunity to the victim in a way that is most favourable to the potential investor. Achievement of the profiled stage, operationalised in the research phase of social engineering, is essential to the overall success in gaining investment from the victim (Workman, 2007a).

Understanding this stage of victimisation and the tactics employed has direct relevance to formulating fraud prevention measures. Individuals need to recognise that when they receive a cold call regarding investment opportunities that those contacting them have already researched them to determine points of vulnerability. The offender has researched the potential investor to determine the most effective way of developing trust and rapport and then uses this to maximise the likelihood that they will solicit a positive response to the investment offer. At this stage, the best fraud prevention measure that potential victims can enact is to discontinue the call immediately before the offender can manipulate the potential victim into becoming involved or interested in the offer.

Relational

The relational stage correlates with the second phase of social engineering, the development of trust and rapport (Mitnick and Simon, 2002; Bakhshi *et al*, 2009), and is enacted in the first stage of boiler room fraud, being the initial cold call. At this stage, potential victims need to be aware that offenders will do whatever is necessary to develop a relationship with them. Offenders will employ a variety of psychological tactics and persuasion techniques to establish trust from the victim. Trust is one of the most prominent factors behind successful social engineering attacks (Peltier, 2006; Okenyi and Owens, 2007; Applegate, 2009). Thompson (2006, p. 222) argues that 'social engineering succeeds because most people work under the assumption that others are essentially honest. As a pure matter of probability, this is true: the vast majority of communications we receive during the day are completely innocent in character'.

In applying this to boiler room fraud, the offender seeks to build rapport and gain the trust of the potential investor. Having already researched the potential investor, the offender will have determined how to expedite the establishment of trust and rapport required (Workman, 2007a). It is unlikely that the offender will try to persuade the potential investor into making a financial decision at this initial stage. Instead, the offender will seek approval to send information to the victim about the potential investment opportunity. This approach is effective because the sending of information may seem harmless given that there is no implied monetary commitment at this stage. However, this is a deliberate and effective ploy that facilitates further contact.

This stage also seeks to build trust and credibility in respect to the investment opportunity itself. This is likely to include (but is not limited to) the production of marketing materials and prospectuses, the creation of false Websites and the provision of referees who will attest to the reputation of the offender and the fraudulent company (ASIC, 2002a, b; ACC and AIC, 2012). Each of these will contribute to the perceived legitimacy of the investment opportunity offered and encourage the potential investor to financially commit. Many potential investors will conduct their own research and due diligence without realising that they are relying on false information created by the offender.

Relevant to fraud prevention, it is essential to educate potential victims of the levers that offenders are using during this stage. At this stage, offenders are seeking to capitalise on the trust that the potential investor has in the legitimacy of the caller and the investment opportunity they are promoting. Potential victims should be aware that once

the relationship is established between the offender and themselves it becomes more difficult to be objective about the process. Further, as the relationship develops, the offender uses each interaction to actively seek out information that allows them to further build the profile of the potential victim. This has relevance to the final social engineering phase, utilisation of information (Mitnick and Simon, 2002; Bakhshi *et al*, 2009), whereby information garnered from the victim is actively used in the victimisation process. Personal information collated by the offender maximises the likelihood that the offender is able to counter any suspicions that the victim may have about the investments and ensure that the specific persuasion techniques they employ will be optimally effective.

Exploitable

Potential victims require an understanding that offenders view them as commodities that are open to exploitation. The exploitable stage is correlated with the third stage of social engineering, the exploitation of trust (Mitnick and Simon, 2002; Bakhshi *et al*, 2009) and the second and third stages of boiler room fraud involving the initial follow-up call as well as continued phone calls. Offenders employ a number of persuasion techniques and psychological tactics to take advantage of the trust established between victim and offender. Many social engineers employ tactics of fear, authority and reprisal to gain compliance (Workman, 2007b, 2008; Applegate, 2009; Abraham and Chengular-Smith, 2010). Fear can operate through the threat of suspension or security breach of an account, or through the promise of a limited offer (known as scarcity) (Workman, 2008). The use of authority is usually coupled with fear tactics, and exploits the inherent nature of persons to submit to authority figures. Social engineers can also appeal to the curiosity, empathy or excitement of an individual about a presented opportunity (Abraham and Chengular-Smith, 2010).

In the case of boiler room fraud, offenders will use a combination of these tactics and techniques to obtain a financial commitment from the victim. Research conducted on transcripts of offenders and their fraud pitches found that across 128 transcripts 1103 influence tactics were identified, with an average of 8.6 tactics used per script (NASD, 2006). Thirteen common tactics used by offenders pitching investment opportunities were identified (NASD, 2006). This analysis reveals that offenders will attempt to overwhelm their potential victim with multiple persuasion techniques (Thompson, 2006) and the choice of approach will be tailored to the specific vulnerabilities and weaknesses of the targeted victim. The effect of using multiple persuasion

techniques is to 'put the victim in a kind of psychological haze that somehow changes what might otherwise be a normal ability to spot and resist persuasion' (NASD, 2006, p. 11).

The final social engineering phase labelled utilisation of information (Mitnick and Simon, 2002; Bakhshi *et al*, 2009) typically involves offenders using personal information to gain unauthorised access to victim bank accounts, computer accounts or computer systems but it also has relevance to the exploitation phase as described here. Its application to boiler room fraud relates to a wider conceptualisation of social engineering tactics, in that the use of personal information facilitates a successful financial commitment from the victim to invest in a fraudulent opportunity. The information leads to a monetary output, rather than simply gaining access to an account or computer system. Therefore, the utilisation of information can be applied across several stages of boiler room fraud, including the initial follow-up call, continued calls and the crisis point.

It is proposed that a clear articulation and understanding of the role and operation of the exploitation phase is crucial in fraud prevention. Its application to the financial literacy curriculum would involve educating investors on the range of tactics and techniques used by offenders. Essentially, education would be clearly focused on expanding the approach of investors beyond the application of their financial knowledge and skills in assessing investments. Investors who seek to proactively protect themselves from financial fraud victimisation also need to actively apply their knowledge of persuasion and social engineering tactics as part of their investment repertoire. It is argued that increasing 'traditional' financial literacy knowledge, defined as knowledge of basic economic and investment principles, simple knowledge of risk and skills in management and accessing financial resources (Malone *et al*, 2010), is not sufficient to effectively protect against the approach of fraud offenders.

Yielding

The yielding stage of the PREY model correlates with the third identified stage of the social engineering framework, exploitation of trust (Mitnick and Simon, 2002; Bakhshi *et al*, 2009), and although it applies to all stages of boiler room fraud it is most notable at the final stage, the crisis point. At this stage, the offender will pressure the victim to continue to invest increasing amounts of money in the investment scheme and will refuse to accept any reasons provided by the victim to stop investing. Further, the offender will typically refuse to accept any request by the victim, for example, the selling of shares, that would lead to the cessation of their involvement in the investment.

This stage is usually initiated as a result of the victim wanting to terminate their involvement in the investment. Once the victim requests liquidation of their investment, whether that be because they simply want to realise their investment returns or because they suspect it is a fraud, the fraud begins to unravel. Offenders will use whatever persuasion techniques are necessary to convince the victim to reinvest their money (likely to be with an additional financial commitment) (ASIC, 2002b). Even if the victim has not yet recognised this as a fraudulent scheme, most victims will at this point become suspicious. However, given the trust and effectiveness of persuasion techniques used by the offenders, some victims will be unable to resist further financial investment, despite their suspicions (ACC and AIC, 2012). The skill of the offender and the strength persuasion being used on the victim throughout the boiler room fraud process maximises the likelihood that many victims will continually yield to the demands and requests of the offender. The skills and targeted tactics used make it incredibly difficult for the victim to cease involvement in the fraud and acknowledge their financial losses (ACC and AIC, 2012).

The relevance of this stage to making positive impacts on achieving better fraud prevention outcomes is difficult as this stage occurs following victimisation. However, what can be drawn from this stage is the importance of reporting financial fraud. Investors who do fall victim to financial fraud should be encouraged to report their experiences to the relevant regulatory bodies and police organisations. Not only does this provide the opportunity to pursue offenders and prosecute them, it is through a better understanding of how the financial fraud process is operationalised by offenders that better preventative mechanisms can be designed and implemented.

Conclusions

In conclusion, the PREY model presented in this article was used to summarise the skills and techniques used by offenders in perpetrating investment (boiler room) fraud. Given research to suggest that financial literacy may not be as effective as previously thought in protecting against fraud victimisation (NASD, 2006; AARP, 2007, 2008; ACC and AIC, 2012), this model seeks to expand the financial literacy curriculum beyond attainment and application of financial knowledge and generic warnings about financial fraud. In order for better fraud prevention outcomes to be achieved, the curriculum needs to explicitly include education on social engineering and persuasion techniques.

The preceding discussion focused on examining the stages of the PREY model and derived specific proactive fraud prevention measures that could be integrated into the content of financial literacy curriculum. It was concluded that investors need to recognise, when they receive a cold call regarding an investment opportunity, that the caller (or offender) has typically already conducted research to determine the particular points of vulnerability for that victim (*Profiled*). Further, once the relationship between the potential victim and offender has been established, it is more difficult for the potential victim to be objective about the interaction and offers being made (*Relational* and *Exploitable*). Continued interactions allow the offender to gather more information about the victim further reinforcing and extending the levers that can be used by them to engage the investor in the fraudulent scheme (*Exploitable* and *Yielding*). Investors who seek to protect themselves against financial fraud need to actively apply their knowledge of persuasion and social engineering tactics beyond the application of their financial knowledge and skills.

Extrapolating from these specific fraud prevention messages, it is also important to acknowledge two key general conclusions about fraud prevention in this context. First, many individuals do not realise the value of their personal information and how this can be used by offenders. An increased awareness of the worth of personal details may deter some individuals from providing this type of information without due consideration and assist in preventing them being as exposed to profiling and targeting by offenders. Second, greater awareness is needed in respect to the transfer to monies overseas, a tactic often used in financial fraud (ACC and AIC, 2012). Once money is sent offshore as part of an investment (or in this case boiler room fraud), the ability of financial institutions, police and/or regulators to recover such monies is extremely difficult; recovery of money is 'not only difficult but unlikely' (Button *et al*, 2009, p. 31). These general conclusions clearly indicate and reinforce that prevention is better than reaction, and that investors need to take steps to prevent or at least minimise the risk of being targeted and experiencing financial loss.

It is important to consider how the proposed fraud prevention educational content proposed here, based on the PREY model, could be integrated into the financial literacy curriculum. Unfortunately, others have concluded that empirical validation of the effectiveness of programmes designed to teach individuals to identify or resist persuasive, particularly deceptive or dishonest, techniques and tactics is limited (Sagarin *et al*, 2002). Despite these difficulties, it is possible to identify a number

of general conclusions that may be useful in guiding how investors can be taught to identify and resist fraudulent, persuasive tactics. Drawing on the empirical work of Sagarin *et al* (2002, p. 528), it is suggested that one effective strategy is heightening investors' awareness of 'undue manipulative intent'. In this case, investors are taught that fraud perpetrators use highly sophisticated persuasion tactics that are designed to exploit even those with high levels of financial knowledge and skill. This approach may be effective as it explicitly and directly challenges those who may be overconfident in their ability to accurately identify fraud due to their level of financial knowledge.

Further, the above discussion that identified potential fraud prevention intervention points for each stage of the PREY model can be taught as decision points for investors. This approach provides investors with general decision points that allow them to have a base or starting point on which to evaluate whether the identified and known tactics of social persuasion and engineering are being used. It allows investors a general framework on which to discriminate between legitimate and fraudulent investment-related approaches (Sagarin *et al*, 2002). Application of rules should be taught experientially within the financial literacy curriculum to enhance the ability of investors to understand the evolving nature of identifying investment fraud, building up not a discrete set of rules but an adaptive approach that can be used dynamically across situations and contexts.

At a broad implementation level, it is suggested that the integration of education on social persuasion and social engineering tactics should, at least as a first step, be focused on specific target groups. As discussed earlier, existing research evidence finds that higher rates of financial literacy is generally correlated with age (ANZ, 2011), and in turn age and financial literacy knowledge is often correlated with higher levels of financial fraud victimisation (NASD, 2006; AARP, 2011). It is proposed that the type of educational content proposed in this article would be highly relevant to a target group with these characteristics and it is hypothesised that it would be positively related to better fraud prevention outcomes. It is likely that the target group described could be effectively engaged via a community education context or alternatively, through their financial advisor. This would require upskilling of community educators and financial advisors on the nature and scope of social persuasion and social engineering tactics in this context.

The concept of PREY provides a framework that operationalises social engineering and persuasion tactics. The PREY model challenges investors to see themselves in the same way that offenders perceive them. Offenders

perceive targets or prey as victims that can be profiled (*Profiled*), manipulated through the development of false trust and rapport (*Relational*), exploited (*Exploitable*) and pressured into yielding to offender demands (*Yielding*). In this article, it has been argued that individuals can be empowered to identify, resist and re-engineer the techniques of persuasion used against them by offenders. In this way, the financial literacy curriculum can actively contribute to a proactive, fraud prevention framework, and in turn assist investors to protect their current and future financial well-being.

Acknowledgements

The authors gratefully acknowledge the support of Detective Constable Michael Kelly, Financial Crimes Unit, Toronto Police Service.

References

Abraham, S. and Chengular-Smith, I. (2010) An overview of social engineering malware: Trends, tactics and implications. *Technology in Society* 32(3): 183–196.

American Association of Retired Persons (AARP) (2007) Stolen futures: An AARP Washington survey of investors and victims of investment fraud. http://assets.aarp.org/rgcenter/consume/wa_fraud_07.pdf, accessed 23 February 2013.

American Association of Retired Persons (2008) Consumer fraud: A 2008 survey of AARP Colorado members' experiences and opinions. http://assets.aarp.org/rgcenter/consume/co_fraud_08.pdf, accessed 23 February 2013.

American Association of Retired Persons (2011) AARP Foundation national fraud victim survey. http://assets.aarp.org/rgcenter/econ/fraud-victims-11.pdf, accessed 23 February 2013.

Applegate, S. (2009) Social engineering: Hacking the wetware!. *Information Security Journal: A Global Perspective* 18(1): 40–46.

Australia and New Zealand Banking Group Limited (ANZ) (2011) Adult financial literacy in Australia, http://www.anz.com.au/resources/f/9/f9fc9800493e8ac695c3d7fc8cff90cd/2011-Adult-Financial-Literacy-Full.pdf.pdf?CACHEID=f9fc9800493e8ac695c3d7fc8cff90cd, accessed 20 May 2013.

Australian Crime Commission (ACC) and Australian Institute of Criminology (AIC) (2012) *Serious and Organised Investment Fraud in Australia*. Canberra, Australia: Australian Crime Commission and Australian Institute of Criminology.

Australian Securities and Investment Commission (ASIC) (2002a) *International Cold Calling Investment Scams*. Canberra, Australia: Australian Securities and Investment Commission.

Australian Securities and Investment Commission (2002b) *Hook, Line and Sinker: Who Takes the Bait in Cold Calling Scams? Canberra, Australia: Australian Securities and Investment Commission*.

Bakhshi, T., Papadaki, M. and Furnell, S. (2009) Social engineering: Assessing vulnerabilities in practice. *Information Management and Computer Security* 17(1): 53–63.

Beaver, K. (2009) Social engineering. *Security Technology Executive* (April): 35–36.

Button, M., Lewis, C. and Tapley, J. (2009) *Fraud Typologies and Victims of Fraud: Literature Review*. London: Centre for Counter Fraud Studies.

Deevy, M., Lucich, S. and Beals, M. (2012) Scams, schemes and swindles: A review of consumer financial fraud research, Financial Fraud Research Center. http://fraudresearchcenter.org/wp-content/uploads/2012/11/Scams-Schemes-Swindles-FINAL_11.20.121.pdf, accessed 23 February 2013.

Gamble, K., Boyle, P., Yu, L. and Bennett, D. (2012) Aging, financial literacy and fraud. Social Science Research Network, http://ssrn.com/abstract=2165564 or http://dx.doi.org/10.2139/ssrn.2165564, accessed 25 February 2013.

Joo, S. (2008) Personal financial wellness. In: J.J. Xiao (ed.) *Handbook of consumer finance research*. New York: Springer.

Lusardi, A. (2012) Financial literacy and financial decision making in older adults. *Journal of the American Society on Aging* 36(2): 25–32.

Malone, K., Stewart, S.D., Wilson, J. and Korsching, P.F. (2010) Perceptions of financial well-being among American women in diverse families. *Journal of Family and Economic Issues* 31(1): 63–81.

Manske, K. (2000) An introduction to social engineering. *Information Systems Security* 9(5): 53–59.

Mitnick, K. and Simon, W. (2002) *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN: Wiley.

NASD Investor Education Foundation (2006) Investor fraud study: Final report, http://www.sec.gov/news/press/extra/seniors/nasdfraudstudy051206.pdf, accessed 25 January 2013.

National Fraud Authority (2012) *Annual Fraud Indicator*. London: Home Office.

Okenyi, P. and Owens, T. (2007) On the anatomy of human hacking. *Information Systems Security* 16(6): 302–314.

Peltier, T. (2006) Social engineering: Concepts and solutions. *Information Security and Risk Management* 15(3): 13–21.

Power, R. and Forte, D. (2006) Social engineering: Attacks have evolved but countermeasures have not. *Computer Fraud and Security* 2006(10): 17–20.

Rusch, J. (1999) The social engineering of internet fraud, http://www.isoc.org/inet99/proceedings/3g/3g_2.htm, accessed 25 February 2013.

Sagarin, B.J., Cialdini, R.B., Rice, W.E. and Serna, S.B. (2002) Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion. *Journal of Personality and Social Psychology* 83(3): 526–541.

Taskforce on Financial Literacy (2010) Canadians and their money: Building a brighter financial future, http://www.financialliteracyincanada.com/pdf/canadians-and-their-money-4-rec-eng.pdf, accessed 25 February 2013.

Thompson, S. (2006) Helping the Hacker? Library information, security and social engineering. *Information Technology and Libraries* 25(4): 222–225.

Workman, M. (2007a) Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology* 59(4): 662–674.

Workman, M. (2007b) Gaining access with social engineering: An empirical study of the threat. *Information Systems Security* 16(6): 315–331.

Workman, M. (2008) A test of security interventions for security threats from social engineering. *Information Management and Computer Security* 16(5): 463–483.