The Scammers Persuasive Techniques Model: Development of a stage model to explain the online dating romance scam

## Monica T. Whitty

## British Journal of Criminology

Whitty, M. T. (2013). The Scammers Persuasive Techniques Model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, 53(4), 665-684.

This study examined the persuasive techniques employed by criminals in the online dating romance scam. Twenty participants were interviewed, including financial and non-financial victims. The paper first examines errors in decision making and finds victims make similar errors compared with victims of other mass marketing frauds. It is also proposes that the near-win phenomenon is useful in explaining why individuals remain in the scam and why some become re-victimized. A model called the Scammers Persuasive Technique Model is developed to highlight the processes involved in the scam. It provides a description of the victim and highlights how criminals groom victims prior to any financial requests. The various stages that follow to keep the victim involved in the scam are highlighted.

The Internet has provided a new space for criminals to scam a much larger pool of potential victims, and arguably ICTs (Information and communication technologies) have created many more problems for law enforcement agencies (Mann and Sutton 1998; Shields 2005). One of the crimes on the rise since the advent of the Internet is fraud. The National Fraud Authority (2012) in the UK estimates that fraud costs in the UK equate to over £78 billion a year, with £3.5 billion lost to mass marketing fraud in 2011. They conducted a nationally representative study of more than 4,000 UK adults and found that in 2011, 1 million (2%) UK adults sent money in reply to unsolicited communication, with just under half being defrauded as a result. They also found that three quarters of UK adults (37 million people) received unsolicited communication in 2011 (the majority sent via email). This study was interested in examining a type of mass marketing fraud that initiates over the Internet, known as the online dating romance scam.

The online dating romance scam emerged around 2007/2008 and has its roots in paper-mail based fraud (Whitty and Buchanan, 2012a). Whitty and Buchanan (2012a) estimated from a nationally representative survey that almost 230,000 people might have been conned by romance fraudsters in Great Britain alone. SOCA (the UK's Serious Organised Crime Agency) claim that losses can range between £50-£240,000 (Whitty, in press). Victims include people of all ages and men are just as likely as women to be taken in by the scam (Whitty\_b). Moreover, these authors found that victims of this scam are more likely to score high on romantic beliefs, in particular, on the sub-scale, idealisation.

Currently, very little is known about this crime and its effect on its victims. In fact, the available literature on the persuasive techniques used by scammers is fairly scant (Lea, Fischer and Evans 2009a). This current study attempted to remedy this lack of attention to mass marketing fraud by examining victims' accounts of their experiences of the online dating romance scam. It aimed to examine the persuasive techniques that scammers employ and considered whether previous theories on persuasion are adequate in explaining why victims are conned by this particular fraud.

#### Anatomy of the scam

The online dating romance scam involves both identity theft and mass marketing fraud. In this scam criminals pretend to initiate a relationship via an online dating site or social networking site with the intention to defraud their victims. Criminals create profiles with stolen photographs and at a very early stage the criminal declares their love for the victim and requests that their relationship move from the dating site to other forms of communication. At a certain point the scammer makes requests for money, which can accelerate to large amounts of money. As with advanced fee fraud, sometimes individuals are persuaded to believe that there is some financial gain for

themselves; however, in the main, they appear to be 'chasing the relationship', rather than the money (Whitty, in press). The fraud ends only when the victim learns and accepts that they have been scammed and ceases to give money.

### Persuasive techniques

Levi and Burrows (2008) note that "[f]ew of the studies on fraud are derived from academic or professional analytical sources" (p.296). There are very few studies that have focused specially on the persuasive techniques employed by mass marketing fraudsters. No theory exists that examines explicitly mass marketing fraud and instead scholars tend to draw from established theories developed by social psychologists and adapt these to mass marketing fraud. Moreover, the few studies that do examine persuasive techniques with regards to mass marketing fraud typically focus on the classic 419 scam.

## Errors in decision-making

Lea et al. (2009a) offer the most comprehensive approach to explaining the psychology of scams (although they did not examine the romance scam). Essentially, they argue that "falling for a scam comes down to errors in decision-making", and "scammers create situations (with their scam offers) that increase the likelihood of poor decision-making" (p.35). They believe that "[d]ifferent kinds of scams in their content and persuasive techniques are more striking than their differences – and they do not exploit all kinds of decision error equally" (Lea et al., 2009b). In their series of studies they found that there were both cognitive (e.g., overconfidence in a specific topic) and motivational (e.g., the scam triggers positive emotions) processes to explain the psychological reasons for responding to scams. They found that the most consistent finding across their studies was 'appeals to trust and authority' (i.e., the use of people or institutions of authority to make the scam appear legitimate) and 'visceral

triggers' (triggers that are employed to make potential victims focus on huge prizes or benefits and imagined positive future emotional states). Another error these theorists claim victims frequently make is the belief that they are acting according to the social norm. Norms, they contend, "can be seen as rules of thumb based on social knowledge: they tell us how we 'ought' to choose, and furthermore how people are likely to choose" (p.25). A comprehensive list of the common errors Lee et al. (2009a) believe victims of mass marketing fraud fall for is summarised in Table 1.

Table 1

Errors in decision making identified by Lee et al. (2009a; p. 24)

Motivational	Cognitive
Visceral influences	Reduced cognitive abilities
Reduced motivation for information	Positive illusions
processing	
Preference for confirmation	Background knowledge and
	overconfidence
Lack of self-control	Norm activation
Mood regulation and phantom fixation	Authority
Sensation seeking	Social proof
Liking and similarity	Altercasting
Reciprocation	
Commitment and consistency	

Some of the errors in decision making theorists have identified are strategies that marketers' use to persuade individuals to purchase their products. Lee et al. (2009a) and Rusch (1999) have proposed that scammers employ classic marketing strategies to con their victims. Lee et al. (2009a), in their empirical investigation,

identified some classic strategies including: scarcity and the foot-in-the-door technique. Scarcity, for example, played a role in many of the scams they examined; that is, presenting offers with time limits. This strategy pushes the person to make a quick decision with little time to think about whether it is an intelligent decision. The foot-in-the-door technique was another successful strategy to draw victims into parting with their money. Essentially this technique, labelled by Freedman and Fraser (1966), explains that people who comply with the first small request are inclined to fulfil subsequent requests because of their urge to remain consistent. Drawing from Cialdini's (1984) work, Rusch identifies a few more classic marketing techniques that scammers might employ, such as reciprocation (giving a small gift in order to receive something back) and social proof (if others are buying into the deal it must be genuine).

# Long-odds gamble

Lee et al. (2009a) also found that there was typically a disproportionate relation between the amount of money the victims hoped to gain and the cost of trying to obtain it. They found that "some people viewed responding to a scam as a long-odds gamble: they recognised that there was something wrong with the offer, but the size of the possible prize (relative to the initial outlay) induced them to give it a try on the off-chance that they might succeed" (Lea et al., 2009b). Victims, in their research, were found to keep their involvement in the scam (or what they believed to be a genuine transaction) private from their family and friends. Lea et al. suggest that they might have been keeping the reality from their 'rational selves'. These researchers found that scam victims were less likely to regulate and resist emotions associated with scam offers. These researchers, however, did not examine romance scams, and

by their own admission, although there are many similarities between different scams, different types of scams can exploit "different error tendencies" (p. 135).

#### Elaboration likelihood model

The Elaboration likelihood model (Petty and Cacioppo 1986) is believed by some (Rusch 1999; Langenderfer and Shimp) to be a useful model to explain why some individuals are scammed by mass marketing fraud. The elaboration likelihood model explains how attitudes are changed via two routes of persuasion: the central route and the peripheral route. The central route process requires a great deal of thought and therefore promotes high elaboration. Peripheral route processes, on the contrary, do not involve elaboration. Instead, individuals might focus on the attractiveness of the source. Individuals who process information using the central route do so because the message is important, and are therefore motivated to employ adequate cognitive resources. Those who use the peripheral route do so for personal reasons or because of the weakness of information channels. Drawing from this model, Rusch contends that scammers rely on the peripheral route, stirring up strong emotions, such as excitement and fear. Victims, he argues, are therefore not likely to attend to cognitive cues. It should be noted that Rusch did not carry out any empirical research to examine whether this theory was supported.

Similarly, Langenderfer and Shimp (2001) have drawn from the elaboration likelihood model. In another untested theoretical paper, they argue that victims of fraud make decision errors. They argue that the scammer creates viscerally oriented rewards, which the victim is likely to have a very high motivation to earn. Scam messages, they contend, address basic needs such as greed (e.g., earning large sums of money). Langenderfer and Shimp believe that when visceral influences are high, individuals who are highly motived are more likely to miss the clues in the message

that would alert them to the scam. More attention is instead placed on the reward aspects of the message. The more the individual focuses on the reward, the less non-reward processing that takes place. Therefore, according to their theory, individuals who are more motivated when presented with more visceral cues are more likely to be conned. In contrast, they argue, that for those who are more motivated, when visceral influences are minimal, it is expected that individuals will focus more on the non-reward message arguments rather than the reward per se. Under these conditions, they believe the individual is more likely to recognise the deception and avoid being scammed. Again, as with Rusch's work, these theories have yet to be tested by carrying out empirical studies.

#### Computer-mediated communication

Although psychological theories are clearly important to draw from to explain why individuals fall victim to scams, theories on CMC (computer-mediated-communication) might also provide a clue. Many scams these days initiate on the Internet and researchers have found that people are often very trusting of information they find there (Whitty and Joinson, 2009). Given that this study was interested in the online dating romance scam, research on the development of online relationships might also prove useful in explaining the success of this scam. For example, in some online environments individuals develop 'hyperpersonal relationships'; that is, more intimate relationships than would be otherwise experienced in face-to-face conditions (Walther 1996, 2007). According to Walther's hyperpersonal theory, receivers idealise partners because of the messages they receive, which they believe demonstrate the similarity in their online partner as well as a highly desirable character. In contrast, senders exploit the technology to selectively self-present aspects about themselves that the other would deem socially desirable. The CMC

features allow one to be strategic in their presentation of self and the CMC environment creates a space where the outside world is filtered out and cognitive resources are instead employed to focus on the online communications.

The aim of this paper was to learn, from in-depth interviews carried out with victims of the online dating romance scam, the types of persuasive techniques that drew them into the scam and ultimately conned them out of money. The theories proposed by previous researchers were examined and applied to the data collected for this study. In addition, this paper considered whether any new theories might better explain why victims were persuaded to part with their money.

#### Method

#### **Materials**

A semi-structured interview was developed for this study. While the basic structure of the interview was adhered to for each participant, because of the unique experience each victim had of the scam and the aftermath of the scam, each participant did not receive the exact same interview schedule. The interviewer asked participants to describe their previous romantic relationships, beginning from their first serious relationship to the point they are currently at with regards to romantic relationships. Participants were asked questions about their relationships to learn if there was anything about their previous relationship history that might have made them more vulnerable to the scam. They were then asked to described the scam in detail and explain why they believe they were persuaded by the criminal to believe the relationship was genuine and for those who were scammed out of money to learn why they believe this happened. Finally, in order to ascertain the psychological impact this crime had on individuals they were asked how this crime had impacted on their lives. This paper reports a sub-set of this study (other papers will focus on the typology of

victims as well as the psychological impact of this crime).

#### Procedure

Participants were recruited via two main methods: either from an introduction from the UK's Serious Organised Crime Agency or participants in a survey study conducted by the author, which examined the typology of victims, volunteered to be interviewed at a later date. Given that postings on an online support group (http://romancescams.org/) revealed that people who had not lost money but who had been taken in by scammers felt they too were victims of this fraud, some victims who had not lost money were also interviewed. All interviews, except for one, were conducted face-to-face at a place of their choosing. Participants normally opted to conduct the interview in their homes, however, some opted a local café at a time when they knew there would be few people present. The only interview not conducted face-to-face was conducted on the telephone – given that the person resided in the USA it was deemed too expensive to travel for this particular interview. Interviews gained an in-depth understanding of the victims' experience and typically ranged from 3 to 5 hours (with breaks in between). Some participants were re-interviewed at a later date to gain further insight or to clarify points.

## **Participants**

In total, 20 participants were interviewed for this study. Names have been changed to ensure anonymity. Thirteen heterosexual women who had been scammed out of money and one who felt she had been scammed but not lost money were interviewed. Two heterosexual men and one homosexual man who had been scammed out of money, two heterosexual men and one homosexual man who had not been scammed out of money but felt victimised were interviewed. Ages of the participants ranged from 38-71 years. The amount of money lost ranged from £300-

£240,000. All participants resided in the UK, besides one who resided in the USA. For some participants the scam had taken place a few years prior to the interview, for others the scam had just ended and for one the scam was still continuing. The 'fake' relationship lasted from a couple of months to 3 years. Some victims were repeat victims (one male had fallen victim over 40 times) falling for the same scam with new criminals. SOCA revealed that there are suckers lists that criminals sell to one another which includes a list of their previous victims (personal correspondence).

The narratives spun by the criminals varied, as did, the length of time for the scam. Some victims after several months of developing a relationship were asked for money for a plane fare to allow the fake persona to visit them and potentially start up a new life with them. The person did not show up and gave various reasons for this, often claiming they were in a car accident on the way to the airport and requiring further financial assistance for their hospital bills. This would follow with further requests for money until the victim learnt they had been conned by the criminal. Other scenarios involved a businessperson urgently needing money for their business with the promise this would be quickly paid back.

Some of the women believed they were communicating with an American soldier working in Iraq. They were told that the fake persona was in love with them, about to finish their service, and wanted to retire by moving to the UK and marry the victim. In the process of the move they asked the victim if they would accept bags containing personal goods for them to take care off, whilst they get ready for their move. After acceptance, the victim received a phone call from someone who claimed to be a diplomat and was looking after her supposed lover's bags. The victim was told that given the flight had been delayed, the diplomatic seals were about to expire and that money was needed to ensure that the bags could still be sent through to the

victim. The victim sent money next to learn they were too late and that the bags had been sent to customs and x-rayed only to find that there was money and gold in the bags. This lead to a series of new reasons why the victim was asked to pay money, including paying money to the fake persona who claimed to have been wounded in Iraq. Some women were asked to go to Ghana to sign documents so that they could claim the money. When they arrived they were kidnapped and brought by men with guns to an isolated room and were left there for a couple of days. Eventually the men with guns showed them some of the money and provided them with a document to sign and they were then released. The women went back to the UK still believing in the con and continued to give money until they were informed by law enforcement that they had been victims of the romance scam.

### **Results and Interpretation**

A thematic analysis was carried out on the data. Previous theories (as outlined earlier in this paper) were examined to determine if they could be utilised to explain why victims were taken in by the scam. The analysis also considered any new themes that emerged from the interviews.

#### **Themes**

The first part of this analysis highlights the themes that emerged in this study that have been hypothesised or found in previous literature on mass marketing fraud. It considers themes under three main headings: errors in decision-making, long-odds gamble, and elaboration likelihood model. The analysis then moves to also consider the stages involved in the scam to help explain why individuals are duped by this scam.

#### *Errors in decision-making:*

The introduction of this paper highlighted the motivational and cognitive errors that are made by victims of mass marketing fraud. This paper now turns to examine whether victims of the online dating romance scam make similar errors.

Person of authority: As highlighted in this paper, Lee et al. (2009a) argued that one of the errors victims of mass marketing fraud make is to trust a person in authority. This study also identified this strategy. In the narrative created for the female victims the 'fake' persona was in each case a person in a position of authority (e.g., army general, successful businessman). For one of the male victims the fake person was a medical doctor. Moreover, the majority of the narratives included additional characters who held positions of authority; some examples include: diplomats, lawyers, doctors, law enforcement and so forth. For the victims, these personas of authority represented someone they could trust. Moreover, the women described these authority figures as attractive and the sort of person who would be highly sought out on a dating site.

- P: Oh he was absolutely charming. I couldn't believe my luck. I mean he would....He made promises that he was getting this big pay-out...when he was coming out the air force... And...he wanted me to meet his people and his base...and we would go down...but he named the base. It was one just outside Westminster. I knew the base, and everything. So I thought it was all very feasible. Erm. So I was preparing for him to come back. His son was at...was studying to be a doctor...at this university in London...[Pam]
- S: Yeah, like a foundation or something like that. Make gas and oil foundation for...whole Europe, or...contact with another country. Very attractive. He was rich, important. [Sue]

Norm activation: As highlighted in this paper, researchers believe that individuals are drawn into giving money to fraudsters if the narrative they are presented with activates a particular norm. Most of the participants in this study were presented with narratives to give money based on scenarios where people ought to be considered to help; for example, helping a sick child, medical bills, university fees and so forth.

Moreover, the person they believed they were forming a relationship with was often described as being vulnerable – potentially priming them to help this person. For example, some came from poor backgrounds, whilst others (many of the fake heterosexual male profiles) despite being wealthy, were emotionally vulnerable, being recently left widowed with a child. In most cases the victim believed they would have the money re-paid and that they were helping because the person, at that time, did not have access to their funds.

Scarce deal/emergency/crisis: Consistent with previous research, another theme that emerged was that of scarcity or an emergency or crises. For the majority of financial victims at some point during the scam there was an urgent need for money with serious consequences for the 'fake' persona if the victim did not pay up on time. For instance, money was needed for diplomatic seals for the fake persona's bags or medical bills after being in a car accident or shot at war.

- *I:* So you gave the £3000 for that, to get the medals and things.
- E: Yeah. To get the parcel. Because when this Diplomat said he'd got stuck coz he'd had to stay there a few more days than he thought... the date stamp had expired on the parcel. Coz it had diplomatic immunity. So the date stamp...so it needed to be re-date stamped. [Elaine]

T: Yeah, he'd been mugged and he'd lost his phone and everything, and what could he do? Could he have some more money? [Ted]

In addition to the crisis, there was often the threat of withdrawing the relationship, if the victim did not pay up. In some cases the criminal became very angry with the victim, threatening to go out with someone else or breaking up the relationship. For example, the following victim stated:

- P: So we broke-up and then emailed me and back and I said to him oh don't be so ridiculous, how can you just switch me off after you've spoken to me...like this, and blah blah blah, so it was all on again. And so I sent the money. [Pam] Reciprocation: In only a couple of cases reciprocation was employed; that is, sending a gift in the hope that the victim would reciprocate by sending the requested money. In the cases where it was used, it typically involved sending the female victims flowers and or a teddy bear. This act generated the required response of sending money.
- A: He sent...he sent...not New Years Eve, but the day before, he sent me...I have never seen such a huge box of flowers. In a vase. In a vase. With two boxes of chocolates and a little teddy bear.
- *I:* So how did that make you feel then?
- A: I was...I couldn't speak...I took lots of photos of them and sent them to him...
- A: One of my friends who'd been a bit...because she was distanced from it, said,

  I can't deny anymore that this guy is genuine....
- A: Ok, so it was at that point...things changed and I started sending money.

  [Ann]

Commitment and consistency: It has been argued that individuals have a deep desire to be consistent (Cialdini 1984). This is especially evident when sales people manage

to successfully persuade individuals to buy their products. Lee et al. (2009) highlight this phenomena with victims of mass marketing fraud, referring to the 'sunk cost effect'; that is, the theory that victims feel that because they have invested so much into the deal already they believe that with just a little more money they will eventually obtain their goal. This 'sunk effect' was also evident with romance scam victims, except that the final goal was often the relationship rather than monetary. Love, liking and similarity: Cialdini (1984) contends that individuals are more likely to be persuaded by someone they like and share some similarity. In this study, most victims were deeply in love with the fake persona, which motivated them to give money. They often saw them as the ideal romantic partner – someone they had hoped all their lives to meet. Moreover, they described the fake persona as describing liking similar hobbies and interests to themselves, which brought them closer together. What was also interesting was the bond that was often felt between the other characters brought into the narrative (e.g., the solicitor, lawyer, diplomat). To give an example:

- E: Yes. There was one, I never forgot it, it was talking about love and rain and how love is, can be like a summer spring, but can be like a stormy, and I thought, and then I just wrote back, and I thought by then, it didn't take him long. It did not take him long. In less than two weeks, I had fallen for him.
- I: So did you feel like he knew you better than anyone had known you...in a way...?
- *E:* He connected to me.
- *I:* On the emotional..?
- E: Yeah on the emotional level...on...my hidden things I like...You know when you're looking for your...soul mate...that's the word. [Elizabeth]

- J: Yeah, well Jim [the diplomat in the story], you know, he's my friend, because I'd spoken to him so much. I felt close to him and I miss his friendship even now.
- I: And did it feel like you two were kind of together against the world in this kind of thing?
- J: Yes, and that's why I continued to help Steve out. [Jane]

  Viscaral influences: As explained earlier in this paper researche

Visceral influences: As explained earlier in this paper, researchers have found that victims of scams often experience visceral triggers; that is, they focus on the prize and imagine positive future emotional states. Participants in this study described euphoric feelings of love at the early stages of the relationship. As the scam progressed, however, they often felt stressed and anxiety and many were striving to regain the euphoric feelings felt at the beginning of the relationship, believing that once the crisis had passed they could finally be united with their loved one. Many had visualised the meeting and a few had organised family events where their family and friends would meet the person of their dreams.

- P: Yeah, and it was lovely. And he would tell me these wonderful stories he wanted to know about my first nightmares as a child...what did I like to eat...what drink did I like...and oh! We had everything. He was going to cook for me, and I found that extremely endearing. Because no bloke I've ever been out with has ever cooked for me, unless it was a bbq....
- P: ... He sent this, the day after I sent the money and it was confirmed, was the next day was supposed to be the day he was arriving back in the UK. Do you know, I dressed myself up to the nines. To that day I still believed there was hope. I went to the airport. I went to the airport! And I thought, you idiot! It

- cost me £50 to get there because of the taxi and everything because of his flight and we were supposed to go to this cocktail party afterwards.
- *I:* And you told people about the cocktail party.
- P: Yes! And he was getting a medal and he would be wheeled off the plane in a bloody wheelchair...and then...Nothing! [Pam]

Lack of self-control/addiction: Some participants described feeling addicted to the relationships and found it difficult to cut off the relationship even when they learnt that it was not genuine. Although, the term 'addiction' is a concept that has been the subject of much debate (see, for example, Foddy & Savulescu 2010; Goodman, 1990, Mathews 2010) it appeared that victims experienced some of the symptoms of addiction, such as salience (where the relationship become the most important thing in their lives), tolerance, (requiring more communication over time), withdrawal symptoms (if the criminal stopped communicating with the victim), loss of control, and reduced involvement (in other social or recreational activities due to the relationship).

J: When you talk to somebody, I've thought about this you know, when you talk to somebody for two hours every night and get a written thing from them everyday. You can live with somebody and not talk to them that much and when it's intensive for a couple of hours, they don't just get up and walk away. It really is intensive and it's like you know everything, they know everything and that's how it is. That's how they get you. That's totally how they get you because you get to the point where you live for that email to come through in the morning. I used to get my email in the morning and MSN at night and that's how it was. That's just how it was. My kids were used to me buried in the

- computer as soon as it came online. It was always roughly around the same sort of time. I felt completely addicted.
- *I: In what way do you feel addicted?*
- J: If he hadn't sent an email or Instant Messenger that day would that have felt painful? I was always waiting for them and I know there was times, especially as it went on, there was times when if there was a bit of a gap I'd be like, "Is he alright? What's he doing?" Then as soon as I got an email it was like [sigh of relief], "That's alright." [Judy]

As mentioned earlier, some victims continued on with the scam even when law enforcement informed them that they were victims. Others moved onto the next scam. It might have been these individuals' addictions that lead them to be repeat victims.

# Near win phenomenon

Earlier in this paper, Lee et al.'s (2009a) view that victims of mass marketing fraud make the 'long-odds gamble' was highlighted; that is, despite holding suspicions that they might be scammed, if they send enough money they might eventually reap the rewards. Similarly, this study identified that some victims do go for the 'long-odds gamble', but in addition the near win phenomenon might shed more light as to why some victims are drawn in to the scam and find it hard to exit accepting their loses. A number of researchers have argued that a near win (or near miss), while gambling might explain why some individuals continue to gamble (e.g., Griffiths 1999). Essentially, a near win is a failure that comes close to being successful, such as three lemons and one orange lined up on the slot machine (Skinner 1953). This strategy was evident in many of the case studies examined in tis study. Near wins included buying airplane tickets for the 'fake persona' believing they

would at last be united, only to be confronted with a mishap or emergency on the way to the airport. For repeat victims, near wins consisted of a fake persona who will hopefully be a real candidate next time along. This was especially the case for some of the men, who invested in small amounts for each fake persona and moved quickly onto the next romance scam.

#### Elaboration likelihood model

As described earlier in this paper, a number of theorists have argued that the elaboration likelihood theory can be used to explain why individuals are conned by various mass marketing frauds. Scam messages are said to contain messages that address basic needs, in this case love. This research found, together with previous research (Whitty & Buchanan, 2012b), that victims of romance scams are more likely to be have 'idealised romantic beliefs'. Therefore, it is likely, that victims pay more attention to the visceral cues related to love. However, although it was evident that the victims interviewed for this study (both financial and non-financial victims) were highly motivated to find a romantic relationship with many falling in love with the fake persona, they nonetheless did not ignore the cognitive cues. For example, victims often requested and were emailed boarding passes, information about the news in the country the criminal was claiming to be living in, fake letter heads and logos stolen from authentic organisations. This means that preventive strategies need to go beyond seeking out simple cues to authenticate a genuine or fake relationship and that the elaboration likelihood model, at least for this scam, does not easily explain why victims are taken in.

H: No. It was the USA government. I wasn't giving him the money. I was giving the money to the USA government, and they sent me a document that X has got

that looked from US government, saying that to have leave, a certain amount of money would have to be released, and he couldn't use his credit card or passport because they take away everything while they were abroad. [Helen]

Although participants were presented with information that could be construed as authentic, and often worked hard at checking the facts, they were often simultaneously presented with information that was clearly not genuine. For example, one victim described thinking that catching Nigerian airlines from Iraq to Amsterdam (where the criminal was claiming to be travelling and managed to present a boarding pass to prove the fact) seemed an odd choice of airline for an American general and did bring to mind the 'Nigerian email scam'. However, when she went to question this, the criminal re-worked the narrative to convince her that a Nigerian Ambassador was somehow involved in the work he was doing. Most victims interviewed for this study reported that at some time during the scam a friend or family member pointed out that they were being duped, and when given examples of other similar cases, dismissed them, believing that their relationship was genuine.

What appears to be happening for this victim, as well as others, is that they worked hard to 'cognitively dismiss' messages that are out of synch with the narrative they want to believe. The theory of cognitive dissonance, developed by Festinger (1957), is of use here. Essentially, this theory outlines that when two opinions, beliefs or items of knowledge are dissonant with each other individuals feel discomfort. Individuals might attempt to reduce dissonance by changing their beliefs and opinions or acquiring new knowledge in order to reach consonance or forget or reduce the importance of those cognitions that are in a dissonant relationship. If people want to reduce the discomfort caused by dissonance they might employ rationalisation to explain away the competing items of knowledge. Some, but not all, of the non-

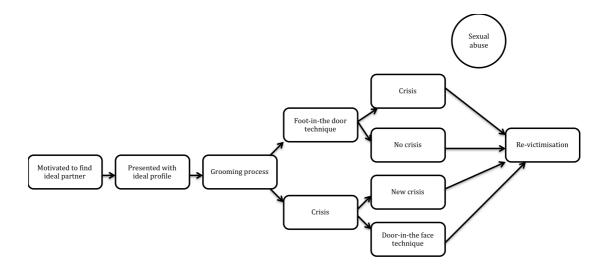
financial victims were more sceptical when presented with conflicting information, which helped prevent them from becoming non-financial victims.

In addition to considering the specific errors in decision making that victims of mass marketing fraud make, it is useful to also understand the scam in its various stages. By viewing the scam in this way, we might be able to better understand where it is that victims are 'hooked in' to the scam and how we might go about preventing the scam.

# **Stage Approach: Scammers Persuasive Technique Model**

The first part of this analysis confirmed many of the themes highlighted by previous researchers who have investigated other types of mass marketing fraud. The near win phenomenon was added as a new theme to explain why some people find it difficult to leave the scam and why some become re-victimised. It was found that the elaboration likelihood model could not fully explain the scam and instead the theory of cognitive dissonance provided a better explanation.

It is contended here that in additional to considering the errors people make that understanding the scam as a process can provide further explanation for how people are persuaded to believe the scam and find it difficult to leave the scam once hooked. The analysis revealed a series of stages, which when carefully orchestrated manages to reel the victim in and eventually develop enough trust with the victim to con them out of money (see Figure 1).



Stage 1: Motivated to find the ideal partner. All of the participants (both financial and non-financial) talked about the hope of finding their ideal partners on the site. Some participants had been single and searching for years, whilst others had only recently moved out of a relationship. One participant, for example, described hoping to find a 'Mills and Boons' type relationship, where she would be swept of her feet.

Participants had different views about the 'perfect' relationship; nonetheless, they all appeared motivated to find this person.

Stage 2: Presented with the ideal profile. Again all participants (both financial and non-financial) described the 'fake profile' they were presented with by the criminal as outlining an ideal person. Ideal did not necessarily mean the Brad Pitts and Angelina Jolie's in the dating world, but rather whom the victims themselves felt was an ideal person for them (sometimes reading between the lines). Not all profiles contained a detailed description of the 'fake persona', however, the cues presented to the victims were enough to draw them in. All of the participants described the photograph as physically attractive. The stolen photographs used to create a female profile often contained pictures of women scantily dressed and looked like a model (probably

because they were stolen pictures from a website of a woman trying to make her way as a model). The stolen photographs used to create a male profile were more varied; however, it was not uncommon to have pictures of men in uniform (e.g., army general). There was often a large age discrepancy between the victim and the person created in the fake profile and in most instances this did not seem incongruous to the victim. Although descriptions of the fictitious person varied, the fake male profile often had the character as someone who was widowed, with a child, in a professional job or a businessman. The fake male profile presented to homosexuals varied between a professional person (e.g., designer) and a student profile, from a poor background. The fake female profile typically presented the character as a poor student or someone in a low-paying job, such as a nurse. The following basic descriptions tap into the typical characteristics that men and women seek in a partner and are therefore a sensible strategy for the scammer to employ. Researchers have found that women look for a partner with high socio-economic status and men look for a partner who is physically attractive (Kenrick, Sadalla, Groth and Trost 1990).

Stage 3: Grooming process. Again all victims entered into the third stage; however, it was this stage that determined whether the victims would be financial or non-financial victims. This stage, I refer to as the grooming stage, given that it shares similar aspects to the way a sexual offender might groom a child. Gillespie (2002), for example, defines grooming as:

The process by which a child is befriended by a would-be abuser in an attempt to gain the child's confidence and trust, enabling them to get the child to acquiesce to abusive activity. It is frequently a pre-requisite for an abuser to gain access to a child. (p.411)

Sex crimes towards children have been described as a process that does not 'just happen', but rather is carefully planned, rehearsed and imagined ahead of time (Lacombe 2008). As Hudson (2005) points out, a sex offender goes through a number of stages leading up to the offence, stages that involve "the use of cognitive distortions and deviant sexual fantasies, and the use of covert and overt planning in order to groom both the environment and the victim (p.39)."

Similar to grooming a child, scammers groom their victims until they are ready to give money. They gain the victims' trust by providing them with a seemingly safe environment to disclose their deepest thoughts, secrets and insecurities (often revealing aspects about their lives that they had opted to not disclose to any other, including previous loved ones).

It is argued in this paper that ICTs are used in the scam to help develop this trusting relationship. Moreover, the strategy of living abroad and the excuses of why it was impossible to meet face-to-face provides the criminal with time to develop a close relationship with the victim. This is in contrast to the typical relationship developed on an online dating site, given that most online daters try to meet their person from the site fairly quickly, often within weeks after initial contact on the site. Little time is spent getting to know one another beyond the profile because individuals want to learn if the profile matches up to the real person (Whitty 2008; Whitty and Carr 2006). This study, however, found that a different type of progression and relationship development occurs when scammers are developing relationships with victims from online dating sites. Instead, they spent much time communicating with them via various modes of communication (in particular email and instant messenger). Unlike other typical online dating relationships, the focus on getting to know one another online was made possible because the loved one

Instant messenger was used to authenticate the relationship and draw the victim close to them. Moreover, by making the relationship a routine part of their life (with morning and evening IM chats) a strong attachment was created making it more difficult to break away from. What become evident in this study is that the scammer was creating a 'hyperpersonal' relationship with the victim (described earlier in this paper; Walther 1996, 2007). The scammer had the time and the knowledge to present the ideal person to the victim.

Walther argues that when people are communicating via ICTs, they become much more focused on the online communications, blocking out other environments. The victims reported continuously re-reading emails and looking forward to the next romantic email or IM chat session. Although adding phone might theoretically increase trust, communicating via ICT leaves a record for individuals to revisit whenever they want – reinforcing the romantic messages being sent by the criminals. ICTs, therefore, help strengthen the relationship making it more difficult for victims to break away from the relationship.

Towards the end of this stage, the scammer might test the waters by asking for a gift, and if they victim complies they move onto the next stage. Stage 4 consists of a number of different routes. This is dependent on the strategy the scammer decides to employ.

Stage 4: The Sting. At this stage the criminal initiates requests for money, either through the foot-in-door technique (described below) or by creating a crisis in the narrative. If the victim had been groomed successfully they complied with giving money, if not they attempted to exit the relationship, whereby the criminal would

revert back to Stage 3 and attempt to continue with the grooming process until the victim was ready to part with the money. Some victims manage to exit successfully and made no further contact with the criminal. For example, the following male non-financial victim exited after the criminal began to be aggressive towards him when he would not comply with requests for money:

M: It was beginning to kind of get a little bit too much, the story, so I started asking more questions, at which point he got more aggressive in the emails and was accusing me of not caring and leaving him up the creek without a paddle and that kind of thing, and playing a lot on the emotional blackmail side of things. [Mark]

Interesting, the resilience of those who were not defrauded out of money cannot be always attributed to knowledge of the scam. For example, one non-financial victim interviewed related that he exited the scam after two weeks of communication, when the scammer said they were on a business trip to Nigeria and needed some money; however, as the interview unfolded it became evident that he was being scammed by another criminal who was claiming to live in Romania (because the scammer took over a year to request money, and he had built up a trusting relationship with them, he felt this was a genuine relationship). This suggests that the more skilful the criminal is at grooming the victim, the more likely the victim is to be taken in by the scam.

<u>Testing the waters/foot-in-door technique:</u> During Stage 4, as mentioned earlier, one of the strategies a criminal might employ is the foot-in-door technique. Victims were asked for requests for gifts or small amounts of money as a way of testing the waters;

from there, if the victim complied, they would be continually asked for more amounts of money.

<u>Crisis:</u> Although the majority of cases reported here demonstrated the criminals employed the foot-in-door technique, others moved immediately to a crisis. This was perhaps because the criminal felt the victim was primed enough to comply with requests for large amount of money. Moreover, the crisis event, means that potential victims are given little time to check facts or their 'gut feelings'. The following victim was groomed for approximately a month when the criminal created a crisis, where she parted with over £90,000 over a weekend:

- F Oh, yeah. Yeah. And how kind and caring I was, and I was the person for him and, the clever bugger, he'd asked me what I wanted to do with my life. I said, I want to live in France. Of course, he says, how much have you got, and I told him.
- *I: Oh, really?*
- F I fell right in that trap, because he said, well, I would like to marry you...
- I: Yeah.
- *F And he wanted to put in the same money and go and live in France.*
- I: Yeah.
- F I was walking on air....
- F I remember I was sitting here and logged on and there was an elongated, "Pleeeeease Help" on Messenger.
- I: And had you, did he ever send you any gifts, or did he ask for anything to be sent to him at any stage?
- F No.

*I:* No? So this was the first request for anything.

F Uh huh. [Fiona]

Stage 5: Continuation of the Scam. The fifth stage again consists of financial and non-financial victims. The criminal employs the door-in-the-face technique (described below) for those who have not complied with money requests for the crisis. Those who complied with the door-in-the-face technique are either presented with a crisis (which was the most common strategy observed in this sample) or they were continually asked for requests for small amounts of money (which might continue over a number of years). Those who were originally presented with a crisis in Stage 3 were presented with a new crisis in Stage 5. Stage 5 continued with new crises or requests for small amounts of money until either the victim ran out of money (and sometimes proceeded to Stage 6) or exited the scam or the victim learnt that they had been scammed (either self-realisation or by being informed by law enforcement, which was in the majority of cases).

<u>Door-in-the face technique</u>: As stated above, when criminals tested the waters with victims, not all victims complied; this lead to a change of tactics, with some using the door-in-the face technique. With this compliance technique the person is first asked an extreme favour that most would refuse, followed by a moderate request (Cialdini 1984).

I So how much did they ask for at first?

F: About £2000, for the airfare.

*I:* And did you give her the money?

F: Only half of it, I didn't have it all.

*I:* Was that ok?

F: Yes she said that she could find half of it after I told her I couldn't afford £2000. (Fred/Sandy)

Stage 6: Sexual abuse. In a few of the cases, after the victim revealed they had no money left to give, the victim hyped up the sexual connection in the relationship and asked the victim to take their clothes off and masturbate in front of the webcam. Victims who complied did so even though they could not see the other person on the other end of the camera. In some cases this was used as a later stage to blackmail the victim, threatening to send the recorded video to victims' work and family. Victims who entered this stage felt incredibly embarrassed and ashamed of their acts, and all reported that they would never have felt comfortable engaging in cybersex with anyone else before and were not sexually adventurous types.

Stage 7: Re-victimisation. Most victims who entered into Stage 7 skipped Stage 6. In the majority of cases, where the victim was informed about the scam by law enforcement, they reverted back to the scam (either back to the same scam or by a entirely new romance scam). Those who reverted back to the same scam were confronted with further requests for money for a variety of reasons. For example, some were emailed by someone claiming to be law enforcement in West Africa (although according to SOCA, this was the same criminal), that they had apprehended the criminal and for a couple of thousand pounds they could release the money stolen by the criminal to the victim. Others were told by the criminal that they had indeed scammed them, but during the process they had genuinely fallen in love with them.

As this new relationship grew the scammer would then ask for further money requests from the criminal.

## Understanding the process

Many of the financial victims reported feeling swept away by the process (what might be understood as a state of 'flow'), whilst others described themselves as feeling addicted. These processes are described below:

Flow: Csikszentmihalyi (1975/2000) first conned the term 'flow' to explain how individuals feel while engaged in intrinsically motivated activities. Essentially, 'flow' is a mental state, where a person is immersed fully in an activity, where they dedicate intense attention and involvement and skill in encountering challenges. He identified nine major components of flow experience: challenge-skill balance, action-awareness merging, clear goals, unambiguous feedback, concentration on the task at hand, sense of control, loss of self-consciousness, transformation of time and autotelic experience. Research has since identified the flow experience being evident in activities, such as sports and exercise (Kawabata and Mallett 2011) and video games (Annie, 2011). In this study, it was found that once the grooming process commenced, victims described becoming fully immersed in the relationship, blanking out other interactions in their lives. Once the Sting began, the challenge for many became obtaining the money to pay the victim (through loans, friends, family) as well as finding a way to send the money (if a local branch at moneygram, for instance, blocked them from sending money). The ultimate challenge for victims, though, was to obtain the relationship that they had been striving to achieve. Victims described being caught up in the situation and in some ways immersing themselves into a world with the

scammer. Although individuals caught up in 'flow' are not necessarily addicted to the experience, it has been suggested that there is a casual relationship between flow experience and addiction (Chou and Ting 2003).

#### **Conclusions**

This paper conducted interviews with victims of the online dating romance scam to learn how criminals manage to persuade victims to believe in their narratives and, for many, part with their money. It draws from previous work that has examined persuasive techniques of mass marketing fraudsters and considers whether these theories apply to this particular scam. Most theories did apply, however, the elaboration likelihood model did not provide an adequate explanation for this scam. Instead, the theory of cognitive dissonance explains how individuals are able to attend to some information and disregard other credible information. The analysis revealed that the near win phenomenon provides further explanation for why some individuals remain in the scam. In addition, a new model called the Scammers Persuasive Technique Model was developed to add to our understanding how the scam progresses. This model explains why individuals get hooked and how criminals manage to carefully groom individuals to a point where they are ready to part with their money. It also explains the initial motivations of the victim that draws them into the scam, followed by the techniques used by the scammer in a carefully set of orchestrated stages to gain trust and eventually scam the individual out of money. This paper contends that it is important to acknowledge the role of ICTs in creating a close and trusting relationship with the victim. Understanding the process as a 'flow experience an addiction for some victims, might also help future researchers comprehend the difficulties victims find in identifying that they have been scammed

and once they have been notified the problems they continue to encounter with exiting the scam.

#### References

Annie, J. S-A. (2011), "I Feel Present. Therefore, I Experience Flow:" A Structural Equation Modeling Approach to Flow and Presence in Video Games', *Journal of Broadcasting & Electronic Media*, 55/1: 114-136.

Chou, T-J., and Ting, C-C. (2003), 'The Role of Flow Experience in Cyber-game Addiction', *CyberPsychology & Behavior*, 6/6: 663-675.

Cialdini, R. B. (1984), *Influence: The Psychology of Persuasion*. New York: William Morrow.

Cialdini, R.B., Trost, M.R., and Newsom, J.T. (1995), 'Preference for Consistency: The development of a Valid Measure and the Discovery of Surprising Behaviour implications', *Journal of Personality and Social Psychology*, 69: 318-328.

Csikszentmihalyi, M. (2000), *Beyond Boredom and Anxiety* (25<sup>th</sup> anniversary ed.). San Francisco: Jossey-Bass (original work published in 1975).

Festinger, L. (1957), *A Theory of Cognitive Dissonance*. Standard, CA: Stanford University Press.

Foddy, B., and Savulescu, J. (2010), 'Relating Addiction to Disease, Disability, Autonomy, and the Good Life', *Philosophy, Psychiatry & Psychology*, 17: 35-42.

Freedman, J. L., and Fraser, S. C. (1966), 'Compliance without Pressure: The foot-in-the-door technique', *Journal of Personality and Social Psychology*, 4: 195-202.

Gillespie, A. (2002), 'Child protection on the internet – Challenges for Criminal law', *Child and Family Law Quarterly*, 14: 411-425.

Goodman, A. (1990), 'Addiction: Definition and Implications', *British Journal of Addiction*, 85: 1403-1408.

Griffiths, M. D. (1999), 'The Psychology of the Near-miss (revisited): A Comment on Delfabbro & Winefield (1999)', *British Journal of Psychology*, 90: 441–445.

Hudson, K. (2005), Offending Identities: Sex offenders' Perspectives of their Treatment Management. Cullompton: Willan Publishing.

Kawabata, M., and Mallett, C. J. (2011), 'Flow experience in Physical Activity: Examination of the Internal Structure of Flow from a Process-related Perspective', *Motivation and Emotion*, 35 (4): 393-402.

Kenrick, D. T., Sadalla, E. K., Groth, G., and Trost, M. R. (1990), 'Evolution, Traits, and the Stages of Human Courtship: Qualifying the Parental Investment Model', *Journal of Personality*, 58: 97-116.

Lacombe, D. (2008), 'Consumed with Sex: The Treatment of Sex Offenders in Risk Society', *British Journal of Criminology*, 48: 55-74.

Langenderfer, J., and Shimp, T. A. (2001), 'Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion', *Psychology and Marketing*, 18/7: 763-783.

Lea, S., Fischer, P., and Evans, K. (2009a), 'The Psychology of Scams: Provoking and Committing Errors of Judgement', *A report for The Office of Fair Trading*.

Retrieved from Office of Fair Trading website:

http://www.oft.gov.uk/shared oft/reports/consumer protection/oft1070.pdf

Lea, S., Fisher, P., and Evans, K. M. (2009b), 'The Economic Psychology of Scams'. International Association for Research in Economic Psychology and the Society for the Advancement of Behavioral Economics, Nova Scotia, Canada, July 2009.

Levi, M., and Burrows, J. (2008), 'Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey', *British Journal of Criminology*, 48: 293-318.

Mann, D., and Sutton, M. (1998), More change in the organisation of thinking. *British Journal of Criminology*, 38/2: 201-229.

Mathews, E. (2010), 'Explaining addiction', *Philosophy, Psychiatry & Psychology*, 17, 23-26.

National Fraud Authority. (2012) Annual fraud indicator.

Petty, R. E., and Cacioppo, J. T. (1986), *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. New York: Springer-Verlag.

Rusch, J. (1999, June 24), 'The 'social engineering' of Internet fraud'. Paper presented at the 1999 Internet Society's INET'99 conference. Retrieved from http://www.isoc.org/isoc/ conferences/inet/99/ proceedings/3g/3g 2.htm.

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: 526-541.

Shields, P. (2005), When the 'Information Revolution' and the US Security State Collide: Money Laundering and the Proliferation of Surveillance, *New Media & Society*, 7/4: 483-512.

Skinner, B. F. (1953), *Science and Human Behavior*. New York: The Macmillan Company.

Walther, J. B. (1996), 'Computer-Mediated Communication: Impersonal, Interpersonal and Hyperpersonal Interaction', *Communication Research*, 23: 3-43.

Walther, J. B. (2007), 'Selective Self-Presentation in Computer-Mediated Communication: Hyperpersonal Dimensions of Technology, Language, and Cognition', *Computers in Human Behavior*, 23: 2538-2557.

Whitty, M.T. (2008), 'Revealing the 'real' me, searching for the 'actual' you: Presentations of self on an internet dating site'. *Computers in Human Behavior*, *24*, 1707-1723.

Whitty, M. T. (in press). 'Anatomy of the Online Dating Romance Scam'. *Security Journal*.

Whitty, M. T., and Buchanan, T. (2012a), 'The Online Dating Romance Scam: A Serious Crime'. *CyberPsychology, Behavior, and Social Networking, 15*(3): 181-183

Whitty, M. T., and Buchanan, T. (2012b), 'The Psychology of the Online Dating Romance Scam'. A report for the ESRC. Retrieved from: http://www2.le.ac.uk/departments/media/people/monica-whitty/Whitty\_romance\_scam\_report.pdf

Whitty, M. T., and Carr, A. N. (2006), 'Cyberspace romance: The psychology of online relationships'. Basingstoke: Palgrave Macmillan.

Whitty, M. T., and Joinson, A. N. (2009), 'Truth, Lies, and Trust on Internet'. London: Routledge, Psychology Press.