

Original citation:

Whitty, Monica T. (2015) Anatomy of the online dating romance scam. *Security Journal*, 28 (4). pp. 443-455.

Permanent WRAP URL:

<http://wrap.warwick.ac.uk/81285>

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions. Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher's statement:

"This is a post-peer-review, pre-copyedit version of an article published in. *Security Journal*. The definitive publisher-authenticated Whitty, Monica T. (2015) Anatomy of the online dating romance scam. *Security Journal*, 28 (4). pp. 443-455.

<http://dx.doi.org/10.1057/sj.2012.57>

A note on versions:

The version presented here may differ from the published version or, version of record, if you wish to cite this item you are advised to consult the publisher's version. Please see the 'permanent WRAP URL' above for details on accessing the published version and note that access may require a subscription.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

Anatomy of the Online Dating Romance Scam

Monica T Whitty

University of Leicester

Dept of Media and Communication

Email: mw229@le.ac.uk

Preprint: Security Journal

The Online Dating Romance Scam is a relatively new form of online fraud. This paper draws from three qualitative studies: an analysis of posts from a public online support group, in-depth interviews with victims of this crime, and an interview with a SOCA officer to outline the anatomy of this scam. It is argued here that there are five distinct stages of this crime. In the first stage the criminal creates an attractive profile to draw in the victim, in Stage 2 the criminal grooms the victim, priming them to send money, in Stage 3 the criminal begins to request funds from the victim (there are four potential trajectories at this stage), in Stage 4, which only a few went through, the victim is sexually abused via cybersex, and finally Stage 5 is the revelation.

Understanding the anatomy of this scam is important for prevention as well as psychological treatment.

Online Dating Romance Scam, Romance scam, mass marketing fraud, scams, internet crime.

The work reported in this paper was supported by award RES-000-22-4022 from the UK Economic and Social Research Council. I would also like to acknowledge the valuable assistance provided by the UK Serious Organised Crime Agency and PARSHIP GmbH.

Anatomy of the Online Dating Romance Scam

The National Fraud Authority (2012) in the UK estimates that fraud costs in the UK equate to over £78 billion a year, with £35 billion lost to mass marketing fraud. Mass marketing fraud essentially exploits mass communication techniques (e.g., email, Instant Messenger, bulk mailing, telemarketing) to con individuals out of money. The Internet has opened up the floodgates to fraud given that criminals can use it to target many more potential victims. Mass marketing fraud is a serious and organised crime. Examples include: foreign lotteries and sweepstakes, 419 scams, charity scams, romance scams, and boiler room scams.

Criminologists have written much on the Nigerian Advance Fee Fraud (also known as the 419 scam, because of the Section number of Nigerian criminal law that applies to it) but there is a scarcity of research available on other mass marketing fraud scams. The Nigerian Advance Fee Fraud actually began in the 1970s as postal mail and faxes and subsequently scammers took advantage of free email and mailing lists to target many more potential victims. In this scam the criminals pretend that there is a large amount of funds that are trapped or frozen for a variety of reasons (e.g., unclaimed estate, corrupt executive, dying Samaritan) and in each case they offer the recipient rich rewards for simply helping government officials or family members out of an embarrassing or legal problems (Whitty & Joinson, 2009).

This paper focuses on one form of mass marketing fraud, the online dating romance scam. In some ways it is similar to advance fraud scams; however, the portrayed end goal for the victim is typically that they will be in a committed relationship rather than simply in receipt of large sums of money. Like the Nigerian email scam it existed as postal mail prior to the Internet (and this form still exists). The postal mail form typically targeted men who purchased adult magazines with

personal ads. The men would write to someone they believed to be a woman who placed attractive photographs with themselves as either naked or very scantily clad (these were of course bogus photographs) with the intention to meet the woman. The criminal would develop a relationship with the victim often sending more photographs and then proceeded to con them out of money.

The Internet Crime Complaint Center (2012) found that, in the USA, The Online Dating Romance Scam was one of the Top 5 Internet scams reported in 2011, with over 5,600 complaints. On average, each victim reported a loss of \$8,900. Action Fraud (2011), in the UK, identified 592 victims, of these, 203 individuals lost over £5,000. According to SOCA (Serious Organised Crime Agency) financial losses can range between £50-£240,000 (personal communication, 2011). These figures, however, are grave underestimates of the prevalence of the crime. Whitty and Buchanan (2012) estimated from a nationally represented survey that almost 230,000 people may have been conned by romance fraudsters in Great Britain alone (and these are the people who are aware they have been scammed out of money). Whitty and Buchanan argue that it is most likely the shame and upset experienced by the victims that deter them from reporting the crime. Action Fraud believes that the number of victims is rising. This seems plausible given that online dating has become a very popular and almost normative activity in Western society. Dutton and Helsper (2007) report that 23% of Internet users in the UK have met someone online that they did not know before. Dutton, Helsper, Whitty, Buckwalter and Lee (2008) found that 6% of married UK couples who use the Internet had met their partner online.

In order to prevent mass-marketing fraud it is essential to understand the framework of each scam. Given the newness of this crime, there is currently no existing publication that outlines in detail the anatomy of this scam. Whitty and

Buchanan (2012) and Rege (2009) provide a sketch of the crime, but not a thorough account. Rege (2009), for instance, drew from websites to devise a basic summary of the scam. The scammer, she claims, contacts the victim and then establishes a strong bond with their victim, which can last from six to eight months. Next she states that the scammer requests money from victims by creating a story of a tragic or desperate circumstance such as theft of personal documents during travel, unexpected hospital funds or request to money to pay for travel expenses to meet the victim. This paper draws from three qualitative studies conducted by the author in order to provide a detailed anatomy of the online dating romance scam.

Methods

Three qualitative studies were carried out in order to learn about: the anatomy of the scam, the profile of the victim, the persuasive techniques the employed by the scammers, as well as the psychological impact on the victim. The results reported here will focus solely on the first objective: the anatomy of the scam. This anatomy is arrived at by examining the victims' perception of the stages as well as a SOCA officer's perspective. Given that those who had lost money to criminals and those who had been duped by a fake relationship but did not lose money, both defined themselves as victims, both types are included in this paper – this helps understand the anatomy of the scam and at what point non-financial victims are not prepared to give money to the criminal. The SOCA officer was an expert on these cases and had spent four years investigating this crime, interviewing criminals who had committed this crime and worked closely with victims. Themes that were mentioned by fewer than 10% of the participants were not included in the results.

Study 1

Study 1 involved collecting 200 posts from a public website. Posts were collected from 50 men and women who stated they were financial victims of the online dating scam and 50 men and women who stated they were non-financial victims of the online dating romance scam. This decision was made given that early reading of the posts revealed that individuals who had not lost money still described themselves as victims, and joined the site to gain support.

Study 2

In Study 2 twenty participants were interviewed. These were in-depth interviews that typically lasted from 3-5 hours. 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. Participants had a range of occupations, from non-professional, to professional jobs or were students or retired. Their economic situations differed, some were less affluent working class individuals, while others were middle class. The amount of money lost did not appear to correlate with their economic situation. 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' relationships lasted from a couple of months to 3 years. A few of the women went to Ghana and were subsequently kidnapped. Names have been changed to ensure anonymity.

Study 3

A two-hour interview was conducted with the SOCA officer who was an expert in law enforcement regarding this particular crime: including in both its postal and online variations. The officer was asked about how he had previously investigated the crime, he's perspective on the stages of the crime (from both interviewing victims as well as criminals), he's observations on the psychological impact this has on victims of this crime, as well as he's suggestions on future interventions to prevent the crime.

Results/Discussion

As illustrated in Figure 1, the study identified four main trajectories of the scam and five distinct stages. According the victims in both studies and the SOCA officer, all trajectories start with an attractive profile that draws the victim into a potential relationship, this is then followed by a grooming process, which can last from a couple of weeks, to several months or even a year. The studies identified four variations of the third stage, but each variation involved requests for money. The following section elaborates on each of these 5 stages providing some explanation for the success of this scam.

INSERT FIGURE 1 ABOUT HERE

Stage 1: The profile

Participants in both studies and the interview with the SOCA officer revealed that the bogus profiles were typically fairly basic with an attractive photograph. For example, the profile contained general details about their hobbies and interests. In most instances the scammer contacted the victim. In some cases the 'fake profile' suggested the dater was from the same area as the victim (later on stating they had to move to another country for work or that this was a place they had wanted to move to). For example, the profile might have claimed the male persona was an American army officer wanting to move to the UK but was currently working in Iraq, or a

businessperson working in Nigeria. In some cases the profile claimed to be the same nationality as the victim or a mixed race and in other cases they described themselves as someone with a completely different ethnicity. The SOCA officer informed the author that the criminal rarely claimed to be Ghanaian or Nigerian, which many of the criminals are believed in reality to be, often living in their respective countries.

According to participants in all three studies, some narratives had the persona as being of a different nationality (e.g., American, German) working abroad. There are some important distinctions between a typical fake male profile and typical fake female profile that are worthwhile pointing out. Moreover, the study found variations between a fake male heterosexual profile and a fake male homosexual profile. The following extracts demonstrate participants' initial reactions over first reading the scammers' profile:

This man was so good-looking, he took my breath away. (female victim, Study 1)

She looked like a model, very attractive (male victim, Study 1)

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. (female victim, Study 2)

He was a general in the army, he's photo looked very impressive (female victim, Study 2)

I: Said she was a Black girl.

V: No, no, no, no. White. When I think of the picture, the picture does look real to the voice. Looking at the face.... [in this case the SOCA officer involved in the case confirmed the criminal was a Ghanaian male].

(male victim, Study 2)

Fake female profile

According to the male victims and the SOCA officer, the fake female profile typically had an extremely attractive photograph (looking like a model). The SOCA officer informed the author that it is suspected that these bogus photographs are of unsuspecting young women who posted photographs on personal webpages hoping for modelling jobs or from social networking sites. The participants in all three studies stated that the women were often described as being no older than thirty years even when the male victims were in their later years (50 years and over). The male victims, although admitting that it was unlikely in real life that they would form a relationship with someone highly attractive and/or with a large age gap, hoped that this was an authentic possibility. In both studies male victims stated that in some cases the profile claimed to be the same nationality as the victim or a mixed race and in other cases they described themselves as someone with a completely different ethnicity (e.g., Romanian living in Romania). They rarely claimed to be Ghanaian or Nigerian. The male victims claimed that the fake profile stated the person was a woman in a low-paying or non-professional job such as a nurse, teacher or a student or a woman with a small business (e.g., selling jewellery). They often described themselves as being poor. They sometimes described themselves as an honest person looking for an honest, trustworthy partner. They sometimes described themselves as a Christian.

Fake male heterosexual profile

According to participants in all three studies, the male heterosexual profile often contained photographs of what was described as a physically attractive male; however, these were typically not to the same extent as the fake female profile. They were typically not pictures of models (although some were) and, as the SOCA officer

informed the author, photographs again were most likely stolen from social networking sites. According to the victims in both studies, there was greater variation in age with the male profile compared with the female profile (sometimes being as old as someone in their 50s). For some victims, the picture was of a man dressed in an army uniform. The victims reported that some of the profiles depicted the man in a professional job, or as a businessman or an army officer (often of high rank). The majority described themselves as being well-off. According to participants in all three studies, the male persona was typically much younger than the female victim and although the women victims stated that it would be unlikely for them to attract such a mate in real life they believed it to be an authentic possibility. According to participants in all three studies, in many cases the scammer's persona was described as a widower with a child (approximately aged 7-14 years) and sometimes described themselves as an honest person looking for an honest, trustworthy partner, and they sometimes described themselves as a Christian.

Fake male homosexual profile

The participants in Study 1 and 2 revealed that the fake male homosexual profile contained an attractive photograph (sometimes of models and sometimes scantily dressed). The participants stated that the male profile was typically described as fairly young (typically no older than his 30s) and there was a mix in professional status, with some in semi-professional jobs (e.g., interior decorators) or successful businessmen, while others were quite poor, sometimes living in poor countries. Again, in some cases the profile claimed to be the same nationality as the victim or a mixed race and in other cases they described themselves as someone with a completely different ethnicity. Again, they rarely claimed to be Ghanaian or Nigerian.

Theoretical explanation

With regards to the fake heterosexual profiles, the criminals are clearly tapping into typical characteristics that men and women seek in a partner, which is a sensible strategy for the scammer to employ. Researchers have found that heterosexual women look for a partner with high socio-economic status and heterosexual men look for a partner who is physically attractive (Buss & Barnes, 1986; Kenrick, Sadalla, Groth & Trost, 1990; Ellis & Symons, 1990; Townsend, 1993). The fake female profiles typically contained physically attractive women and women in need of support. The fake male profiles typically depicted someone of high socio-economic status in a professional job, who was often well educated and wealthy (the scammer claimed they could not get access to their funds and when they did the victim would be paid back). Their needs were more often emotional needs (e.g., the stressors involved in being left widowed and having the sole responsibility for looking after their child). The research of homosexual attraction is rather slim (Dillon & Saleh, 2012), with researchers finding that gay men rank physical attractiveness as highly important in a potential mate (Bailey, Kim, Hill & Linsemeier, 1997). This was again reflected in the findings from Studies 1 and 2.

Stage 2: Grooming

During the second stage, according to many of the participants' accounts in all three studies, the criminal arguably grooms the victim, increasing the intimacy in the relationship until they believe that the victim is ready to part with their money. The amount of time this stage takes varies for each victim. One victim, for instance, parted with approximately £70,000 over a weekend after knowing the 'fake romantic partner' for about a month; others took over a year to part with their money.

Within a week to a couple of weeks of meeting the victim on the site, the

scammer declared their love for the victim and requested that the relationship move from the dating site to email and IM (Instant Messenger).

She said she loved me and asked me to marry her, so we were talking about a long-term commitment relationship in the first few weeks. (male victim, Study1)

The fake relationships sometimes moved to including text messages and the telephone or VoIP (note: voices can now be disguised using phone apps). Moreover, sometimes more photographs would be sent (often 'photoshopped'). Emails would typically contain poetry (often plagiarised) and declarations of love and Instant messenger were used frequently throughout the day to assist in building a close relationship. Webcams were sometimes used but only one-way with the scammer not providing a visual of themselves.

He sent me a love poem every morning and we were on chat (IM) for hours every night and he called in the morning to say good morning and every night to tell me he loved me and would never let me go. (female victim, Study2)

The victims in both studies claimed during this stage, to have self-disclosed very intimate details about their life history, often telling the scammer more about themselves than they have disclosed to any other. When asked whether they felt the victim had disclosed equal amounts the victims often reflected back to realise that they had self-disclosed greater amounts than the criminal. Victims often described this part of the relationship as very therapeutic.

We were on chat for hours every night and he called in the morning to say good morning and every night to tell me he loved me and would never let me go (female victim, Study1)

During this stage the scammer led the victim to believe they wanted to see them but were delayed for various reasons (e.g., service in the army needed to be extended; business still required them to be physically there; could not afford the plane ticket). It is during this stage that the scammer claims to love the victim and hopes for a committed, permanent relationship. The victim also often claimed to have fallen in love with the criminal or was very committed to the possibility of spending the rest of their lives with them (often making declarations of their love and commitment to family and friends).

According to some of the victims in both studies and the SOCA officer in Study 3, towards the end of this stage the scammer sometimes requested gifts (e.g., perfume, mobile phone), most likely as a testing-the-water strategy. In one instance, a victim in Study 2 was reluctant to send gifts and so their scammer sent her a bunch of red roses (this technique motivated the victim to comply with further requests). This stage of the scam arguably primes the individual to give money to the criminal. As this study found not all victims were prepared to give money and managed to avoid being financial victims, but many were still left traumatised and emotionally devastated. Those who were not conned out of money either realised that it had been a ruse or else were unable to give money and did not realise they were a victim of the scam until the authorities informed them.

Next came the teddy bear with a banner on its chest stating "I Love You."

(female victim, Study1)

We spoke for a week when I got my first bouquet of beautiful red roses.

(female victims, Study 1)

Turning victims into criminals

Levi (2002) defined money laundering as “In essence, it encompasses any concealing of the proceeds of drug trafficking (or other serious crimes) beyond putting the loot visibly on the bed or in one’s domestic safe” (p.182). There were a handful of victims that did not send money, because they had none to send, but continued their involvement, which according to Levi’s definition would be understood to be money laundering. According to the SOCA officer, the victims send money (often unknowingly) to other victims’ accounts to be transferred to others until it lands in the criminals account. This is carried out in order to make it more difficult for law enforcement to trace the money. This, he said, is more typical of the Nigerian version of this scam. The criminal would tell the victim that they needed to transfer their money to another account so they could access it. In some cases financial victims were also asked to money launder. They would be asked to transfer money for the criminal and sometimes told they could keep a portion for themselves to demonstrate that the criminal was beginning to pay back the money they owed them. It is difficult to know from the data collected in these studies whether victims were aware they were engaging in criminal activities.

Stage 3: The Sting

Stage 2 primed the individuals to be ready to give their own or else launder money. Stage 3 is when the criminal attempted to con the victim out of money. If they failed at their first attempt they might continue grooming the victim and make another attempt later on. There were four trajectories identified in the third stage. The trajectories most possibly varied according to the strategies employed by the scammer or what strategies the scammer felt would work best to con the victim out of money. According to participants in all three studies, in most cases the money was sent via Western Union or Moneygram (given that the money is untraceable). The four

trajectories identified are summarised below. Non-financial victims at some point during this stage worked out that this was a scam and did not give money to the criminal.

Trajectory 1: Small amounts to a crisis

In the first potential scenario, the criminal asked the victim for small amounts of money before requesting large sums of money, which then lead to a crisis in the narrative (i.e., the criminal created a scenario where money was needed urgently to deal with a crisis, such as a medical problem). This trajectory was the more frequently reported scenario. For instance, a couple of the financial female victims interviewed were asked to pay for money for the renewal of diplomatic seals for bags belonging to the scammer (approximately £1000), which were waiting transfer to the UK from Ghana. They were given a limited amount of time to pay the money (approximately 24 hours). The stories were varied, and the SOCA officer had noticed changes in the story over time.

I went back to Steven on IM and Steven asked to pay. He said £2,500 for 2 seals. He said he couldn't do this from work because it was for a private business....There was no time to think as I had 1.5 hours to get the money to Jim. I was told I had to do this with moneygram. I ran to the bank and got an overdraft from the bank. I had no ID so I had to go back home and then to the post office. It had to be done so quickly. I then phoned Ghana and got no reply. I was given 1.5 hours to do this and I did this in an hour. (female victim, Study 2)

And then she said, I'm coming over, I want the airfare...And she sorted all out the prices and everything herself. As I say, she didn't arrive because she had this accident and ended up in hospital over there. (male victim, Study 2)

Others were asked to pay for laptops or mobile phones as the criminal told the victim they had these stolen and were unable to find replacements in the countries they were residing. Some of the male victims were asked for small amounts of money to pay for books for the 'fake female's' education or tuition fees or plane fares (so that they could at last meet face-to-face).

If the victim complied with these first requests for money or gifts then the criminal increased the amounts of money requested. This sometimes occurred at a rapid pace and for others it occurred more slowly until the scammer invented a crisis that required urgent funds (e.g., a car accident, medical operation, a sick child, business needing urgent money as the workers were on strike). For example, the female victims who paid for the 'diplomatic seals', were then told that the money had not been transferred quickly enough and given this delay the seals had transpired. They were then asked to pay larger amounts to deal with customs. This then led to the bags being x-rayed to find gold and large sums of money in the bags, which would be lost if they did not pay large sums of money to keep them (£20,000). At this point the victims believed they would get a share in the money and their relationships sometimes moved from chasing both the relationship and the money (for some it moved solely to chasing the money). The crisis in each scenario would escalate and if the victims continued to comply, new scenarios were invented to con them out of money.

In each case the victim believed that the money would lead to a reduction in the amount of time they have to wait until finally meet face-to-face (which is ultimately the real prize for most of the victims). Most of the female victims were led to believe that eventually they would be refunded as the 'fake male' partner was believed to be wealthy and they required the funds simply because given the country

they were residing in they could not currently access the money. With some of these scams a third party was brought into the narrative; according to the SOCA officer, this is believed to be the Ghanaian version of the scam. For instance, in a couple of the scams the criminals ‘doctor’ called the victim telling them their lover needed funds for medical bills. In other cases lawyers and diplomats were involved in the narrative. This made the scam appear more believable to victims and it also provided new ways for the scammer to request further funds.

Some of the female victims who believed they were dealing with wealthy men, were subsequently told by the ‘fake male’ partner that the money they had earned (or contained in the bags they were sending to them) was not entirely acquired via legitimate means. This led the victim to feel they would be incriminated if they reported any suspicions to the police and helped keep the victim involved in the scam and not question any suspicions they might have as they felt they were involved in potentially criminal activities.

In the scenario where the victim believed they were chasing bags of money held in Ghana some of the victims were asked to visit Ghana where they were subsequently kidnapped. The money was said to be in their name and they were asked to sign a statement declaring the money was not acquired via the sale of drugs, firearms or other illegal means. In some scenarios the persona claimed they had also made it to Ghana and so the victim believed they would at last meet. When the victim went to Ghana they were met by an assortment of characters (e.g., diplomat, lawyers, men with firearms). They were often locked in a house for several days until men with firearms showed them some gold bullion and money (as a way to prove the gold and money really existed). The victims signed the forms and then returned home. Some at this point realised they were being scammed; however, the majority

continued to send money until they had no more to give or were informed by the authorities that they had been scammed.

The technique used in this trajectory is a technique often used by advertisers or sales people. It is known as the *foot-in-the-door technique* (Freedman & Fraser, 1966). Sales people for instance might ask the customer to pay for a small amount of money towards an investment or a product and when the customer complies with this request then ask them to invest more money or offer them more products in the deal. Cialdini, Trost and Newsom (1995) argue that people who comply with the first request are inclined to fulfil subsequent requests because of their urge to remain consistent. In our victims' cases there is more than consistency that is the pull, but also the desire to maintain their relationships. Moreover, compliance with the first request (an investment in the relationship) could be understood to signify a greater commitment to the relationship, making it more difficult to say no to further requests.

Trajectory 2: The crisis

For some victims the criminal moved immediately to a crisis without any small requests of money. This might have been for the same crisis as identified in Trajectory 1. Most common immediate crises 'occurred' where the 'fake business partner' claimed the scammer had been in an accident or that their child had become ill or their business was in urgent need of money. Akin to for Trajectory 1, the crisis escalated, and if the victim continued to comply, new scenarios were invented to con the victims out of money.

When she called me 4 hours later she told, that she had been in an accident, hurt a little girl, which was in hospital in a coma. (male victim, Study 1)

His daughter got hurt in an attack by some militants and he asked me for money for medical bills. (female victim, Study 1)

I got a email from her family lawyer saying her inheritance of the gold of 600 kg she has need 600 pound so it can be cleared in my name... (male victim, Study1)

Trajectory 3: The crisis to a decrease in requested funds

In some cases the victim did not comply with requests by the criminal for money from a crisis. In these cases the criminal would then proceed to request smaller amounts of money than originally asked. For example, they might have told the victim that they had acquired some money for their emergency medical expenses but still required a sum from themselves to help out. Once the victim agreed to the smaller amounts of funds the criminal proceeded to find new reasons for why they needed money. This technique is also employed by sales people and advertises and is known as the 'door-in-the-face' technique. With this compliance technique the person is first asked an extreme favour that most would certainly refuse. This is then followed by a moderate request (Cialdini, 1984). Although this is an intentional technique used by sales people, it appeared to be more of a back-up strategy for the scammers.

He started asking for \$2,000 and it has been whittled down to \$300. He always seems to come up with a portion of what he needs and just needs me to bridge the gap. (female victim, Study1)

Trajectory 4: Small amounts of money

Some victims never encountered a crisis in the narrative presented by the criminal. Instead they were asked frequently for small amounts of money. For example, some of the men, in particular, would send the 'fake partner' money for an airplane ticket and they were told that they had to use the money for other more important matters (e.g., bills or university tuition). They would then be told they needed more money for bills or university tuition and later on asked again for money for an airplane ticket.

For others, there was a continued use of the 'door-in-the-face' technique, where amounts of money were decreased until the victim complied. This type of scam appeared to often last for a couple of years (although not necessarily earning any greater amounts of money for the criminal).

Stage 4: Sexual abuse

When the scammer had taken as much money as they could from the victim, in a few instances they humiliated them further by asking them to perform sexual acts in front of the webcam (although this was not reported by the majority of participants). In each instance, the victim did not see the fake person on the webcam. This can occur after any of the trajectories evident in Stage 3. The SOCA officer believed the motivation for this was either for the scammer's own amusement or to use the material later for blackmail purposes. None of the participants in these studies stated that they had been blackmailed; however, this does not exempt the possibility.

Stage 5: Revelation

At some point the victim learnt that they have been scammed. Non-financial victims either skip Stages 3 and 4 or exit Stage 3 fairly quickly to arrive at the Stage of revelation. For financial victims, in some cases victims came to the realisation themselves and sought out evidence to support their hunches (e.g., speaking to the embassy, police, dating company, media). In many cases, the victims were informed by the authorities (after having tracked down the criminal or because a suspecting friend had reported the crime to the police). Once the victim learnt that they have been scammed they were devastated – not only because of the loss of money but also because the loss of a loved one (akin to experience the death of someone close to them). Moreover, as reported in other papers developed from this research, participants reported feeling deep shame and humiliation leaving them unmotivated to

report the crime, believing that law enforcement would feel the same. Furthermore, as reported earlier in this paper, some believed they were in part involved in a crime (money laundering) and so, for this reason, refrained from reporting the crime. Some of the victims reported feeling more upset by the loss of the relationship than the loss of money (even though they had mortgaged their houses for the criminal).

Second wave of the scam

Revelations about being a victim of this crime did not necessarily put an end to the scam. The individual found it difficult to reconcile that the relationship was not real and all participants found it difficult to accept that the image of the person they were falling in love with was not connected to the words written to them or the narrative that unfolded before them. One financial female victim sought out the bogus person behind the photograph (hoping to emotionally connect to what she now knew to be a scammer). Others found it difficult to believe that the scammer did not have real feelings for them.

Given this disbelief it is not surprising that after the scam appeared to be complete a second wave of the scam sometimes took place, where the scammer revealed that they had scammed the victim but had really fallen in love with them. In one case a second occurred when the scammer contacted the victim and pretended to be a police officer in Africa. The victim was told that the scammer had been arrested and for a certain sum of money they would return the money conned from them.

Conclusions

The model presented here provides an outline of the anatomy of a fairly unique scam – in that it involves the deception of a relationship as well as a scam to lose money. Very few studies have made an attempt to delineate the stages involved with mass marketing fraud, and despite the apparent uniqueness of this scam, it may well be the

case that other scams have similar trajectories – in that a trusting relationship needs to be developed with the criminal prior to the actual sting for money. Although the narratives for each victim varied with different excuses to take money from them, nonetheless the anatomy developed here can be used for preventative strategies for law enforcement and dating sites to alert potential victims of this scam. If potential victims recognise some of the stages here then this might help them stop and think before they decide to part with their money. Of course, one of the obvious lessons for victims is not to send anyone they have met online any money. However, a further tip might be (given that the grooming process primes victims so successfully) is to insist on meeting anyone they met on an online dating site within a month at the latest from initial contact on the site – if the dater finds reasons why this is not possible then the individuals should move on to consider other potential dates. Finally, support agencies and organisations (e.g., Victim Support) and health professionals treating victims of this crime could benefit from the results set out in this paper as they need to be aware the details of this scam in order to understand the ordeal the victim has endured

References

- Action Fraud. (2011) Retrieved from: <http://www.actionfraud.org.uk/>
- Bailey, J.M., Kim, P.Y., Hills, A., Linsenmeier, J.A.W. (1997). Butch, femme, or straight acting? Partner preferences of gay men and lesbians. *Journal of Personality and Social Psychology*, 73, 960-973.
- Buss, D. M. and Barnes, M. (1986) Preferences in human mate selection. *Journal of Personality and Social Psychology* 50: 559-570.
- 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.
- Dillon, L. M., & Saleh, D. J. (2012). Sexual strategies theory: Evidence from homosexual personal advertisements. *Journal of Social, Evolutionary, and Cultural Psychology*, 6(2), 203-216.
- Dutton W.H. and Helsper E. (2007) *The Internet in Britain*. Oxford: Oxford Internet Institute, University of Oxford.
- Dutton W.H., Helsper E.J., Whitty M.T., Buckwalter, G. and Lee E. (2008) *Mate Selection in the Network Society: The Role of the Internet in Reconfiguring Marriages in Australia, the United Kingdom and United States*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1275810
- Ellis, B. and Symons, D. (1990) Sex differences in sexual fantasy. *Journal of Sex Research* 27(4): 527-555.
- 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.

- Internet Crime Complaint Center (2012) 2011 Internet Crime Report. Retrieved from:
http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf
- 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.
- Levi, M. (2002). Money laundering and its regulation. *The Annals of the American Academy of Political and Social Science*, 582, 181-194.
- National Fraud Authority. (2012) *Annual fraud indicator*.
- Rege, A. (2009) What's love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology* 3(2): 494-512.
- Townsend, J. (1993) Sexuality and partner selection: Sex differences among college students. *Ethology and Sociobiology* 14: 305-330.
- Whitty, M. T. and Buchanan, T. (2012) The Online Dating Romance Scam: A Serious Crime. *CyberPsychology, Behavior, and Social Networking* 15(3): 181-183.
- Whitty, M. T. and Joinson, A. N. (2009) *Truth, Lies, and Trust on Internet*. London: Routledge, Psychology Press.

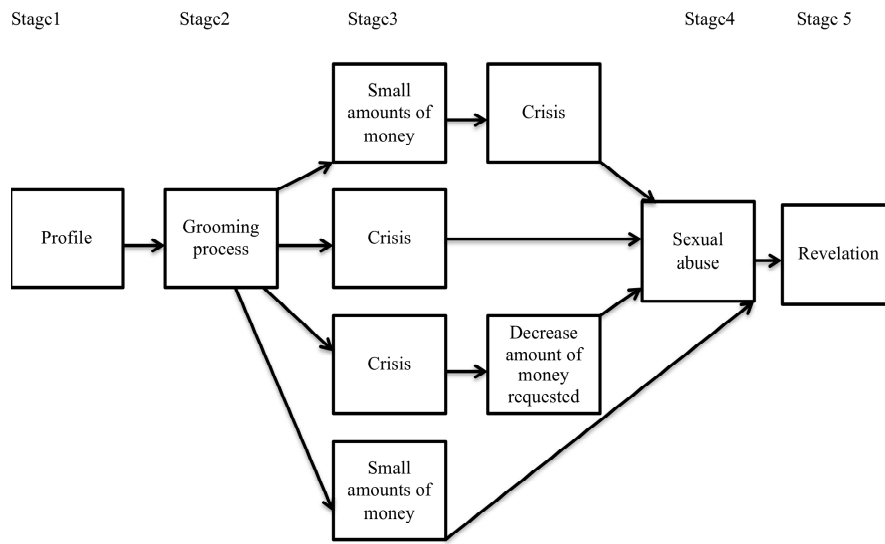


Figure 1 Romance Scam trajectories