Spring 2017

"I Made a Choice": Exploring the Persuasion Tactics Used by Online Romance Scammers in Light of Cialdini's Compliance Principles

Aaron K. Archer
Regis University

“I MADE A CHOICE”: EXPLORING THE PERSUASION TACTICS USED BY ONLINE ROMANCE SCAMMERS IN LIGHT OF CIALDINI’S COMPLIANCE PRINCIPLES

by

Aaron Archer

A Research Project Presented in Partial Fulfillment

of the Requirements for the Degree

Master of Science in Criminology

REGIS UNIVERSITY

May 4, 2017

Abstract

Online romance scams cause a disproportionately high amount of loss to victims when compared to other cybercrimes, and evidence suggests these scams may be more pervasive than official figures indicate. Unlike some other cybercrimes, an online romance scam is only successful to the extent that the scammer can persuade the victim to carry out requests. In his book, *Influence: The Psychology of Persuasion,* psychologist Robert Cialdini has identified six psychological principles often exploited by those seeking to gain the compliance of others; these principles may provide a good framework for understanding the effectiveness of the tactics used by online romance scammers. The study described in this paper sought to accomplish two goals. The first was to identify common themes related to the persuasion tactics used by online romance scammers through an analysis of first-hand stories told by victims. The study identified a number of key themes regarding what victims were led to believe by scammers during the course of the scam. The second goal was to discuss these findings within the context of Cialdini's compliance principles. The study's findings have potential implications for victims and their family members, social workers, members of the financial industry, social media, and law enforcement. It is hoped that a better understanding of how online romance scammers exploit victims' psychological weaknesses will promote a culture of support for victims, and encourage greater attention to be given to this serious and devastating crime.

TABLE OF CONTENTS

Introduction

Crimes committed using computers and the Internet have become ubiquitous in recent decades. From highly sophisticated network intrusions to the most low-tech cyber-stalking cases, the media is permeated with stories about how the Internet is used by criminals to steal money and information, launder money, and commit other crimes. One of the most lucrative areas of cybercrime involves online scams, as evidenced by the fact that, in 2015 alone, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center received complaints totaling over $1 billion. Scams perpetrated over the Internet can target organizations or individuals, and may take on a seemingly limitless variety of forms. However, of all cybercrimes reported to the FBI in 2015, the second highest amount of loss was attributed to a category of fraud that exclusively targets individuals: "Confidence Fraud/Romance" (ICCC, 2016, p. 16). Disturbingly, evidence suggests this type of fraud may be especially underreported by victims, and that the actual financial impact of this crime is far greater than what is indicated by official sources (Whitty & Buchanan, 2012a).

But, unlike with many other scams, victims of online romance scams lose far more than money. Victims of this type of scam are psychologically abused, often for months or even years. Victims have reported experiencing damage to relationships, and being left heartbroken, embarrassed, and deeply humiliated (Whitty & Buchanan, 2012b). During the recent trial of a romance scammer (who was ultimately convicted of defrauding victims of over $1.7 million), victims testified they had filed for bankruptcy, lost jobs, homes, and had been subjected to extreme financial hardship. Beyond their financial loss, victims testified they had fallen into depression and, in some cases, had contemplated suicide. Some victims even testified that they were sexually abused, and later blackmailed using nude photographs of themselves. The

disturbing details of the case, which involved hundreds of victims, prompted the judge who presided over the case to refer to the scam as "the most devastating crime one could ever imagine without laying hands or even eyes on another human being" (DOJ, 2017, par. 10).

A startling feature of online romance scams is that the perpetrators of this type of crime rely on techniques designed to cause victims to act, of their own volition, in ways that go against their interest. To put it another way, unlike some other cybercrimes, such as identity theft, an online romance scam is only successful to the extent that a scammer can persuade a victim to carry out requests. This may help explain why many victims have reported they blame themselves for what occurred, and that, rather than receiving support, they have been met with anger from family members and others (Whitty & Buchanan, 2012b). But what would cause a person to obey the requests of a scammer who may be located hundreds, or even thousands of miles away?

Psychologist Robert Cialdini has identified six psychological principles often exploited by those seeking to gain the compliance of others. Cialdini has discussed these principles at length in his landmark book *Influence: The Psychology of Persuasion*, first published in 1984 and later revised in 2007. Over the years, this book has become required reading in many marketing courses, and has also been retooled into a college textbook, now in its fifth edition. The compliance principles outlined by Cialdini may be a useful framework within which to understand the extreme influence perpetrators of online romance scams have over their victims.

To this end, the study described in this paper sought to accomplish two goals. The first was to identify common themes related to the persuasion tactics used by online romance scammers through an analysis of first-hand stories told by victims. The second was to discuss these tactics in light of Cialdini's compliance principles. An overview of the methodology employed, and ethical considerations, together with the outcome of this research and an exposition of findings

within the context of Cialdini's principles, are outlined below. But before moving into the details of the study, it is helpful to understand the phenomenon of online romance scams against the backdrop of literature that relates to this type of crime, and to provide an overview of the compliance principles outlined by Cialdini.

Literature Review

Attempts have been made to understand the modern phenomenon of Internet-based scams from a number of different perspectives. One approach has been to try to determine the prevalence of the problem, by either trying to ascertain the number of victims or the number of fraudulent solicitations. For instance, a study conducted by the Federal Trade Commission (FTC) found that 10.8 percent of U.S. adults had been the victim of some type of fraud in 2011. In nearly one-third of these cases, the Internet was cited as the means by which the scam was initially promoted (Anderson, 2013). Another study, which involved over 2,300 subjects aged 40 and older, found that 80% of respondents had been the target of a fraudulent offer, and that the Internet was the largest single source of these offers (FINRA, 2013).

With regard to online romance scams specifically, the FBI has reported that, in 2015, its Internet Crimes Complaint Center received 12,509 complaints related to "Confidence Fraud/Romance" scams (ICCC, 2016). However, others have suggested data such as these, which are dependent upon victims self-reporting, may dramatically under reflect the true scope of the problem. For example, a British study conducted by Whitty and Buchanan (2012a) included asking subjects "whether they had lost money or knew someone personally who had lost money to an online romance scammer" (p. 5). These findings, based on a representative sample of adults in the United Kingdom, have led Whitty and Buchanan (2012a) to estimate that over 230,000 British citizens may have been victims of online romance scams between 2008 and

2011. This number is far higher than those self-reported by victims to consumer protection agencies in the U.K. during the same period (Whitty & Buchanan, 2012a).

In the United States, there are a number of ongoing efforts to collect data that include information related to the monetary loss sustained by victims of scams. For example, since 1997, the FTC's Consumer Sentinel project has collected consumer complaints of various kinds, including those related to scams. Between 2013 and 2015, over four million of these complaints related to fraud, with consumers reporting over $4.1 billion in loss. Of fraud-related complaints, 31% of victims indicated that the Internet or email was the method by which they were initially contacted by fraudsters (FTC, 2016). The FBI also collects information specifically related to Internet-based crimes through its Internet Crime Compliant Center. In 2015, the FBI reported that "Confidence Fraud/Romance" represented the second-largest fraud type by victim loss, with victims reporting to have lost over $203 million. On average, victims of this type of fraud reported a loss of $16,260 (ICCC, 2016).

While this amount may seem shocking, a theme throughout the literature related to Internet-based scams is the problem of under-reporting by fraud victims. Different studies have estimated the rate of victim reporting to range anywhere from 1% to 55%, depending on the type of scam and victim demographics (Button, Lewis, & Tapley, 2009; Deevy, Lucich, & Beals, 2012). At least one study found that less than one-third of confirmed fraud victims had reported the crime to authorities, and that a large number even denied they had been victimized when directly asked (Pak & Shadel, 2011). Various factors contributing to the phenomenon of under-reporting have been suggested. For instance, Deevy, Lucich and Beals (2012), based on their analysis of a number of studies, have posited that victims often feel too embarrassed to report the crime, or do not see any benefit in reporting it. Further, victims may be confused about what is

meant by “fraud”, may not know where to report, or may even forget about the fraud incident (Deevy, Lucich, & Beals, 2012). With regard to online romance scams, Whitty and Buchanan (2012a) have found evidence to suggest these scams may be especially underreported. The reasons for this may have to do with the unique characteristics associated with this particular type of scam: “Victims of this scam, unlike any other, receive a ‘double hit’ from the crime; the loss of monies and a romantic relationship. It may well be that the shame and upset experienced by the victims deters them from reporting the crime.” (Whitty & Buchanan, 2012a, p. 7).

Another area of focus has been to try to identify the source of Internet-based scams: who the perpetrators are, and where they are physically located. Longe and Osofisan (2011) have contested the widely-held belief that most advance fee scams originate from West Africa, based on a study of IP addresses associated with scam emails. The study, which incorporated a sizeable percentage of emails classified as “dating spam”, found that a large quantity of scam emails originated from places outside West Africa, such as Europe and North America. However, Longe and Osofisan (2011) have acknowledged their study did not entail investigating whether this pattern “is correlated with the number or volumes of Africans, Asians and other immigrants’ moving into the [sic] western nations” (p. 24). Others have concluded that a superabundance of Internet-based scams perpetrated outside West Africa is, nevertheless, perpetrated by West African-based scammers. For example, Ultrascan (2014), a Dutch security firm that collects and analyzes data related to advance fee scams, has noted West African perpetrators of advance fee fraud (often referred to as “419”, in reference to a section of the Nigerian penal code) have migrated throughout the world in recent years: “There are 419 cells in nearly every country on earth… 419er operations are on the uptick in China (both mainland China and Hong Kong), and in Malaysia. There are 419er cells in the USA, Canada, Mexico, Ghana, Brazil, Egypt, Russia,

India, Pakistan, and the Czech Republic" (Ultrascan, 2014, p. 15). Online romance scams, which Ultrascan (2014) considers a variant of traditional advance fee fraud, are one of the scams routinely perpetrated by West African scammers operating throughout the world.

Yet another approach to the study of this topic has been to explore the possible risk factors associated with the victims of these types of scams, and/or to attempt to better understand victim susceptibility to persuasion techniques used by fraudsters. For example, a study conducted by the AARP identified key differences between the levels of education and income of victims of different types of scams. For example, victims of investment scams were found more likely to be college-educated, and to report an income of $50,000 per year or greater. Conversely, victims of lottery scams were found to have no college education, and to report an income of less than $50,000 per year. The study also examined respondents' susceptibility to a set of marketing-style questions, and found those 50 years and older were "significantly more interested in the persuasion statements overall" (Pak & Shadel, 2011, p. 38). With regard to online romance scams, a series of studies conducted by Whitty and Buchanan (2012b) have suggested that men (whether heterosexual or gay) may be more likely than women to become victims when using an online dating site. Whitty and Buchanan (2012b) have also noted that victims of online romance scams tend to report they fell in love quickly, in contradistinction to studies demonstrating most real romantic relationships mature more slowly; this has led them to theorize that many online romance scam victims are "highly motivated to fall in love, potentially leaving them vulnerable to be scammed" (p. 11).

In another study, Whitty (2015) has examined the patterns that often characterize the progression of online romance scams. Based on a series of qualitative studies, Whitty (2015) has identified five distinct phases of the scam, some of which are characterized by techniques used to

gain the compliance of victims. In the first phase, scammers make adept use of online profiles to entice victims after initiating contact. These profiles often incorporate a photograph of an attractive person, but with significant differences noted between male and female profiles. For instance, heterosexual female profiles often describe the subject of the profile as poor, or as having a low-paying job. Conversely, heterosexual male profiles often describe the subject as financially secure, having a professional occupation, or being a high-ranking military officer. Whitty (2015) has suggested these differences reflect a deliberate effort, on the part of scammers, to leverage distinct factors that men and women typically look for when seeking a romantic relationship. Other phases of the scam include "grooming" the victim, prior to asking for money, and "the sting" – the point at which the victim is asked for money, or is asked for other favors by the scammer (Whitty, 2015).

Overview of Cialdini's Compliance Principles

Given that the victims of online romance scams essentially agree to cooperate with the requests of scammers, it may be easy to adopt a callous attitude toward those who have fallen prey to this type of crime. However, the fact that these scams are so prevalent, and so successful, suggests it is wrong to attribute the actions of victims to stupidity or naiveté. Instead, an effort should be made to understand why the tactics used by online romance scammers are able to cause victims to act in such extreme ways. By illuminating the way in which romance scammers exploit known psychological weaknesses, it may be possible to not only develop better approaches toward mitigating this type of crime, but to also promote more sympathy for victims.

Cialdini has outlined six psychological principles that are often exploited by people seeking to gain the compliance of others, whether for legitimate or illegitimate purposes:

Reciprocation. People are more likely to comply with a request when they feel a sense of obligation or indebtedness toward the requestor. This sense of obligation may be achieved

through giving small gifts or doing perceived favors for someone, but may also be accomplished through *reciprocal concessions:* starting with a large request, then countering with a comparatively smaller request when the first is rejected. This leverages the tendency for people to feel an "obligation to make a concession to someone who has made a concession to us" (Cialdini, 2007, p. 37).

Commitment and Consistency. After making an initial commitment, people often feel constrained to continue to act in accordance with that commitment, in order to "justify [their] earlier decision" (Cialdini, 2007, p. 57). People tend to adapt their self-image to commitments they believe they have made, particularly when those commitments are written down, recorded, or formally made. This propensity is especially strong when a person believes he or she has chosen to make a commitment "in the absence of strong outside pressures" (Cialdini, 2007, p. 93).

Social Proof. People are more likely to conceive of behavior as normal, and to engage in that behavior, if there is a perception that others are doing the same thing.

Liking. People are more prone to comply with the requests of someone they like. Liking can be attained through any number of means, but often includes physical attractiveness, cultivating a sense of "sameness" (people tend to like people they perceive as being similar to themselves), compliments, familiarity, and developing a sense of mutual cooperation toward a shared goal.

Authority. Compliance is easier to obtain when it is perceived that the requestor is in a position of authority. This principle was perhaps most famously illustrated by Stanley Milgram's obedience experiments.

Scarcity. People are often influenced to make decisions based on the fear of losing a perceived opportunity. The perception of scarcity creates a sense of urgency, leading to errors in judgement when people respond by making decisions quickly. This principle owes much of its strength to a concept known as *psychological reactance*: "…whenever free choice is limited or threatened, the need to retain our freedoms makes us desire them… significantly more than previously" (Cialdini, 2007, p. 245).

Methodology

In order to accomplish the first goal established for the present study – identifying themes related to the compliance tactics used by online romance scammers – first-hand stories related by victims of online romance scams were collected and analyzed. Because these stories involved the free-form relation of details in a relatively unstructured context, a qualitative research method was employed; thematic analysis was applied to the stories in order to identify tactics used by scammers. As noted above, compliance is obtained from romance scam victims not through physical force, but through persuasion. The qualitative approach employed for this research enabled the collection and analysis of those details romance scam victims themselves believed to be most important. The freedom to express the details of their ordeal, together with their thoughts and feelings, provided a rich repository of information which might facilitate a better understanding of the compliance techniques used by scammers.

The stories that were used for this research were obtained from a public, online blog where romance scam victims were encouraged to share details regarding what happened to them. For this project, 82 victim stories were selected from responses posted to the blog between December, 2014 and December, 2016. Since the premise of the blog is to assist victims of online romance scams, all posts in which a user recounted the details of his/her story were assumed to be examples of online romance scams, and were considered when making selections for the

research sample, except under the following circumstances: 1. posts which contained clear indications that the scam did not begin over the Internet, 2. posts where the user recounted details of a scam involving someone other than him/herself, 3. posts that did not contain a coherent narrative or other substantial details related to the scam that took place, 4. posts by the blog moderator, or 5. posts which represented responses to other posts, and which did not include the user's own account of being scammed.

The information required for this research was obtained through an analysis of the victim stories that were collected. The 82 selected stories were copied and saved into a Word document in order to ensure the sample remained static during the course of the research. Posts (excluding those matching the criteria referenced above) were then individually copied into an Excel spreadsheet, together with each corresponding post number and date. This format allowed the stories to be easily cataloged, analyzed, and annotated. A thematic analysis of the stories was then conducted, with an emphasis on identifying themes related to what victims were told by scammers. First, an initial, careful reading of all stories was conducted to identify any recurring themes. During this first phase, potential themes were noted, and each was assigned a category heading. Next, a second reading of all stories was conducted in order to denote the stories in which each theme occurred.

Ethical Considerations

The research that was conducted for this study was predicated upon information disclosed by victims of a terrible crime. A primary aim of this research was to yield information that will aid the effort to mitigate romance scams and that might provide a better understanding of what victims endure. With that in mind, this study only used information disclosed by victims voluntarily, to a public Internet blog. A major goal of this approach was to ensure that the research data were obtained only from victims who were ready to share the details of their stories openly, and to disclose those

details they believed were most relevant. The research conducted for this study did not entail the use of live subjects, as defined under federal regulations (CFR, 2009).

In addition to the fact that these victims chose to share their stories publicly, the majority of them did so under obvious pseudonyms, effectively hiding their true identities. Often these monikers appeared to describe the victim's feelings or the details of his or her ordeal (e.g., "lost and hopeless", "Broken Soul", "Scared and sad", etc.); in other cases, the names that were chosen were more prosaic, but equally anonymous (e.g., "lou", "lyoung123", "Luzpi", etc.). In a few examples, names appeared less like monikers, and might have been the victims' true names; however, because users could choose whatever name they liked when posting, it was not possible to know whether any names were genuine or aliases.

Results

Analysis of the stories told by victims identified a number of notable themes with regard to the persuasion tactics used by scammers. Primarily, these themes related to the occupation and appearance of the scammer, proposals of marriage and/or allusions the scammer made to the permanency of the relationship, details related to the scammer's current marital and family status, and tragedies and/or emergencies that had supposedly befallen the scammer. Other themes were also identified that, while less common, nevertheless appeared pervasive. These included victims being led to believe that other people (besides themselves) were also involved with helping the scammer, victims being led to believe they would receive a material reward, and scammers making threats or giving ultimatums to victims.

In a majority of the victims' stories, they specified how they first came into contact with the scammer, and the scammer's purported occupation. Of those victims who specified the mode of first contact, more than half indicated they had met the scammer through a dating site (e.g., Match, Eharmony, OkCupid, etc.). The remainder of victims predominately indicated they met the scammer through other social networking sites/applications such as Facebook, LinkedIn, and Tinder; a handful

of victims also specified other platforms, such as Craigslist and Skype. Of victims that indicated the occupation of the scammer, most said that they were led to believe the scammer held a high paying and/or high-profile job. The main scammer occupations mentioned by victims included engineer, military, and contractor/business owner.

Victims often described the profile pictures used by scammers as featuring someone extremely attractive and/or apparently affluent. For example, one victim described her initial encounter with the scammer in the following way:

> "This guy found me on LinkedIn and sent me a message about wanting to get to know me [as] more than a friend... It took me at least a couple of days to reply because I was not sure if this [was] real or some kind of trick… So seeing this message made me feel important, noticed by this gorgeous 55 [year] old man who happens to be a chief engineer..."

Another primary theme involved proposals of marriage made by the scammer, or the scammer making allusions to the permanency of the relationship. Not surprisingly, most victims indicated they were led to believe the scammer would eventually come to be with them, in person. However, a number of victims mentioned that, within a relatively short time, the scammer either explicitly proposed marriage or otherwise began to speak about the relationship as being permanent. In some cases, victims stated that the scammer even began to refer to the victim as his or her spouse (e.g., referring to the victim as "wife"). Interestingly, another primary theme involved the ostensible marital status, along with other biographical facts, related to the scammer.

A large number of victims mentioned that the scammer claimed to be widowed or divorced. In many cases, scammers seemed to link this aspect of their biography with elements of past tragedies: spouses had died in car accidents, of cancer, or while in childbirth; divorces had been rocky, or ex-spouses had taken all the scammer's money. In other cases, elements of past tragedy

were woven into the scammer's biographical narrative in other ways. For example, in several cases victims were led to believe the scammer's parents had been killed, leaving the scammer an orphan at a very young age. Many victims also mentioned that the scammer claimed to have one or more children; in some examples, the children were also integrated into tragic narratives involving death, illness, or accidents. The following are examples taken from two different victim stories, and illustrate how these themes were often related by victims:

> "He said he moved from McLean, VA, had a wife who died in a car crash four years ago with a seven-year-old daughter named Rachel and recently moved to Southern California..."

> "He said he's a Structural Engineer at Arab Contractors in the greater New Orleans area…. He took his six-year-old son to Cambodia with him but told me his son died after complications from appendicitis."

While the above examples relate to tragedies which had supposedly occurred in the scammer's past, many victims also recounted dramatic events which they were told befell the scammer during the course of the relationship. A large number of stories referenced various accidents or emergencies which the scammer claimed had occurred at some point after the victim's relationship with the scammer had started. In many cases, these circumstances became the apparent pretext by which the scammer first asked the victim to send money or take other specific actions: businessmen were detained by customs when travelling internationally and had to pay fees in order to be released; military personnel found themselves "stuck" in foreign countries when the army refused to pay them; lovers who had suffered injuries in car accidents languished in hospitals and needed help paying medical bills. Victims often described elaborate plotlines, with numerous twists and turns, frequently requiring victims to assist at different points along the way.

Nevertheless, many victims indicated that, after the relationship was initiated, the scammer often waited for a relatively long period of time before asking for any favors. At least one victim even related that she had initially volunteered to help the scammer without being directly asked. Another victim said she chatted with the scammer for six months before he initially asked for money: while supposedly on his way to visit the victim, he was detained at the airport for failing to declare $30,000 in cash – a customs official had confiscated the cash, and payment was now required to facilitate the scammer's release. One victim, who said she ultimately lost her entire retirement savings to the scam, described a similar scenario with regard to how she was first asked for money by the scammer:

> "[He was] leaving Iran and was flying to Calgary, via Dallas Fort Worth. Because he brought some of his equipment with him, customs in DFW detained him and said that he would need to pay them to bring the equipment to Canada as they said it was 'contraband'. I was given bank accounts in Canada to deposit money into – as the U.S. customs officer had friends in Canadian customs who would help him. Eventually he made it to Calgary and was detained again... He needed more money. After I had paid, a day or two later he contacted me to say they deported him as the money that was paid was not enough."

Another victim, who had gone as far as packing her belongings in anticipation of moving into a house together with the scammer and his son, described the circumstances under which she was first asked for help by the scammer:

> "He said when he retired, the army doesn't pay his way and [he] needed help getting a plane ticket… [Later] another major crisis popped up. There was a $5,000 payment he had to pay the army before he could leave the country, he said his friend could

> deposit the money into my bank then I could send the money to him and I could keep $300."

The above example also illustrates two minor themes identified in victims' stories that, while less common, were identified in multiple examples. First, several victims mentioned they had been led to believe that people besides themselves were helping support the scammer financially and in other ways. In some of these cases, victims said the amount for which they were asked was relatively smaller than the amount supposedly being provided by others. For example, one victim said the scammer told her he needed money for expenses related to a business project. His family was already sending him $7,000, but he still needed $3,000. Another victim said that the scammer, who claimed to be in the military, begged her to send him money so he could travel home. He asked her for a relatively small amount, and said he could get the rest of the money he needed from his friends. It was noted that, in general, many victims recounted being contacted by a variety of people apart from the scammer him/herself, all of whom supported the scam narrative, and most of whom apparently pressured victims to send money. These individuals ranged from supposed friends and family members of scammers to a host of others, including attorneys, immigration officers, and doctors.

Secondly, some victims mentioned that they were offered a material incentive to provide assistance or send money to the scammer. In many of these cases victims said they were told the scammer had sent them a gift, and that the gift had been sent via courier. In at least one case, a victim indicated that she had actually received a teddy bear, flowers, and chocolates in the mail. However, in most cases, victims said that after they were told the package containing the gift had been shipped, they were informed that a deposit or other fee had to be paid before it could be delivered. Some victims described the contents of the supposed package. For example, one victim mentioned that she was told the package contained an engagement ring; another said she was shown photographs of expensive jewelry and designer handbags. In some cases, victims said they were told packages

contained large sums of cash. Interestingly, in these cases this seems to have become the pretext for asking the victim to pay a fee: because customs agents had discovered a large amount of cash inside the package, taxes or fees were now required to have it released and delivered to the victim.

A closely related theme involved the scammer claiming to have received a large financial windfall, and asking for help paying taxes and fees necessary to obtain it. In many of these cases, victims indicated that they were led to believe they, too, would benefit from the windfall. One victim, who said he lost over $150,000 to the scam, described how he was told the scammer needed help obtaining an inheritance:

> "After a month or so [the scammer] started asking me to help her to get her inheritance from her deceased father who was murdered by his business partners in Australia. I told her I would help her if it wasn't too expensive… [she] kept pumping me telling me she would pay me back every penny with high interest if I would just stick with her."

A final minor theme identified in victims' stories involved the use of threats or ultimatums made to victims, especially when they hesitated or refused to send money to scammers. For example, one victim said the scammer told her if he couldn't meet her in person by December, he would end the relationship. Another victim said that, after not sending money to the scammer for four months, the scammer "punished" her by only chatting with her once per day. Some victims even described how the physical wellbeing of the scammer was used as a threat. For instance, one victim said she was told by a "friend" of the scammer that the scammer had fallen into a coma due to stress about his financial situation (a situation which the victim was being pressured to help remedy). Another victim described how the scammer even threatened to commit suicide when she refused to send more money to have a supposed parcel delivered to her:

> "I told him I'm broke without money… He told me he is hurt by me and told me not to text him until I settle the matter… he told me if the parcel cannot [be delivered] he will jump into the sea and let me feel regret my whole life…."

Discussion

The information contained within victims' stories provides a wealth of information related to the techniques online romance scammers use to coerce and manipulate victims into complying with their demands. The themes that emerge through the analysis of such stories suggest that successful tactics are repeatedly used by scammers, and that some tactics may be used more often than others. It is clear from victims' stories that these tactics are often incredibly effective – many victims indicated that they lost substantial sums of money, often over long periods of time, as the result of complying with the demands of scammers. As further testimony to the success of scammers' tactics, though many victims alluded to having sustained a significant financial loss, they tended to emphasize the greater emotional loss they felt in the wake of the scam. Many victims expressed feelings of deep despair, depression, and heartache; some even indicated that they still felt an emotional attachment to the scammer, and a few mentioned that they had experienced thoughts of suicide.

Additionally, it is clear from statements made by victims that most viewed their actions as entirely voluntary, and connected the results of their actions with choices they had freely made. Many associated this fact with a deep sense of shame, guilt, and embarrassment. One victim summarized her feelings this way:

> "…I feel like an idiot. I feel ashamed, embarrassed and am completely heartbroken. After coming from a very unhappy marriage, I thought I'd found the man who I was going to spend the rest of my life with. I believed everything he said. I could have said no at any time… but I believed him. He played me – I see that now. He used and betrayed me in one of the worst possible ways. Both the police and the therapist I've

> been talking to have said this wasn't my fault… but who else is to blame? I allowed this to happen. No one forced me. I made a choice – based on the information I had at the time… Although I'm going to continue therapy it doesn't take away my shame, my embarrassment and [my] guilt for not saying no. They say time heals all wounds and I believe that to be true. It will take me years to rebuild my finances. How long does it take for a broken heart to heal though?"

In order to understand the enormous power of the persuasion tactics used by online romance scammers, it is helpful to consider them within the context of Cialdini's six compliance principles: reciprocation, commitment and consistency, social proof, liking, authority, and scarcity.

Many victims said they were led to believe the scammer had sent them a gift; many also indicated that the scammer had proposed marriage, or made other statements which suggested the relationship would be permanent. As was noted, in some cases these themes even converged, as in the case of the victim who believed the scammer had sent her a package which included an engagement ring. According to Cialdini (2007), the principle of *reciprocation* is predicated upon the tendency of people to comply with the requests of someone to whom they feel a sense of indebtedness: "Most of us find it highly disagreeable to be in a state of obligation. It weighs heavily on us and demands to be removed… For this reason alone, then, we may be willing to agree to perform a larger favor than we received, merely to relieve ourselves of the psychological burden of debt" (p. 35). A victim who is led to believe that a scammer has purchased him or her an expensive gift, and/or that the scammer has made a life-altering commitment to the relationship, might feel more obligated to act when later asked for favors.

But proposals of marriage and the offering of gifts may accomplish more than one objective from a scammer's perspective. These acts might serve as signs of commitment on the part of the scammer, potentially placing the victim in a state of obligation – but they also require commitment

from the victim (e.g., accepting a marriage proposal, agreeing to accept gifts, and/or initially agreeing to pay small fees associated with gifts). This dynamic corresponds closely with the principle of *commitment and consistency*: "Once we have made a personal choice or taken a stand, we will encounter personal and interpersonal pressures to behave consistently with that commitment. Those pressures will cause us to respond in ways that justify our earlier decision." (Cialdini, 2007, p. 57). In order for a scammer to leverage this psychological principle, it is integral that an initial commitment be secured from the victim. According to Cialdini (2007), this principle is particularly effective when commitments are made in written form (as would naturally be the case with email or many other electronic mediums), or when a person believes the initial commitment was made of his or her own volition. This could explain the tendency of scammers to initially abstain from asking for money while simultaneously claiming to have experienced various emergencies or accidents; a victim who volunteers to intercede may be even more likely to comply with subsequent requests.

Against the backdrop of scammers claiming to have experienced accidents, emergencies, and other dramatic circumstances that scammers often communicated to victims, many victims mentioned that the scammer also told them other people were already "helping". Many other victims referenced having been introduced to other supposed persons who corroborated the scammer's stories, and/or encouraged victims to provide assistance. The persuasive power of such tactics can be explained within the context of the principle of *social proof.* According to Cialdini (2007), "We view a behavior as more correct in a situation to the degree that we see others performing it… Usually, when a lot of people are doing something, it is the right thing to do" (p. 116).

At times, it seems scammers may leverage the power of social proof together with other techniques. For instance, in addition to being led to believe that a host of others were also helping the scammer, some victims indicated that, compared to the others who were supposedly assisting, the amount they were asked to provide was smaller. This tactic may exploit the psychological principle known as *perceptual contrast,* which is especially strong when two things are presented in succession

(e.g., when a victim is told that "a friend" is lending $7,000, but the victim is asked for $3,000). As Cialdini (2007) has summarized: "Simply put, if the second item is fairly different from the first, we will tend to see it as more different than it actually is" (p. 12).

It is important to note that all the persuasion techniques employed by online romance scammers necessarily occur within the broader context of assumptions victims formulate when they first encountered a scammer. As was noted, a majority of victims indicated they met scammers through dating websites, or other social networking media. Victims often mentioned that the profile picture used by the scammer featured someone who was very attractive, and/or apparently affluent. Significantly, physical attractiveness is a major component of the *liking* principle: "Research has shown that we automatically assign to good-looking individuals such favorable traits as talent, kindness, honesty, and intelligence. Furthermore, we make these judgments without being aware that physical attractiveness plays a role in the process" (Cialdini, 2007, p. 171). In addition to luring potential victims, and corroborating a scammer's claims about him or herself, an attractive profile picture may also serve to increase a victim's likelihood of complying with later requests.

Scammers may further enhance the effectiveness of the liking principle through the various facts they communicate to victims about themselves. For example, many victims mentioned that the scammer claimed to be widowed or to have gone through an extremely difficult divorce. Perhaps not coincidentally, many victims also mentioned that they, themselves, were widowed, were having marital problems at the time they became scam victims, or had been through difficult divorces. Cialdini (2007) has noted that people are more predisposed to like someone they perceive as being similar to themselves. If a scammer can initially lead a victim to believe that the two of them have had shared or similar life circumstances, this might help leverage the power of the liking principle even more.

Many victims also related that the scammer claimed to be trying to obtain a large sum of money, or was actively engaged in some other type of important endeavor that required victims' help

and cooperation. According to Cialdini (2007), "Compliance professionals are forever attempting to establish that we and they are working for the same goals, that we must 'pull together' for mutual benefit, that they are, in essence our *teammates*" (p. 185). As the result, leading victims to believe they are cooperating with the scammer toward a shared goal might also help leverage the power of the liking principle. It is worth noting again that many victims indicated they were led to believe that the "help" they lent to the scammer would ultimately serve them both, either implicitly or explicitly.

Along the same lines, many victims stated that the scammer claimed to hold a position normally associated with a high level of skill, education, and/or status. The tendency of people to comply with the requests of a person in a perceived authority position has been well-documented and, as Cialdini (2007) has noted, was classically illustrated by the experiments of Stanley Milgram. According to Cialdini (2007), one of the primary ways the authority principle is leveraged as a compliance technique is through the use of titles: "Titles are simultaneously the most difficult and the easiest symbols of authority to acquire. To earn one normally takes years of work and achievement. Yet it is possible for somebody who has put in none of this effort to adopt the mere label and receive a kind of automatic deference" (p. 222). Significantly, many victims specifically mentioned the scammer's job title (e.g., "Chief Engineer", "Marine Engineer", "Electronics Technician", etc.), suggesting that the title was an important part of the scammer's supposed identity.

Finally, many victims said they were, at various points, led to believe the scammer had experienced an emergency of some kind, or that their action was otherwise immediately required in order to obtain something, or to prevent something bad from happening. Implicit or explicit limited timeframes were often associated with these emergencies. For example, if money was not sent immediately, the scammer would be deported, the package containing a gift would not be delivered, or some harm might befall the scammer. Cialdini (2007) has noted that the "deadline tactic" is often used to exploit the principle of *scarcity*. Strictly speaking, the scarcity principle leverages its power from the fact that "as a rule, if [a thing] is rare or becoming rare, it is more valuable" (Cialdini, 2007,

p. 239). But the scarcity principle may be employed just as effectively when someone is made to feel he or she has only a limited time to act in a given situation. The fear of losing an opportunity increases the chances of making errors in judgement, causing people to act in ways that might otherwise go against their reason. Additionally, a number of victims indicated that the scammer made ultimatums, or otherwise threatened to cutoff or limit the relationship, unless the victim complied with the scammer's requests. Leading victims to believe that the very relationship itself could be jeopardized because of delayed action might exaggerate the effect of this principle.

Limitations and Conclusion

The goals of this study were to identify themes related to the persuasion tactics commonly used by online romance scammers, and to explain those tactics in light of Cialdini's compliance principles. To achieve these goals, stories told by victims were collected and analyzed. However, there were some limitations inherent in this approach. First, victims' stories were posted in a free-form context, to a public blog, where victims only shared the details they chose. This resulted in inconsistency with respect to the quality and content of the data. In many cases, victims went into great detail regarding their experiences; in other cases, victims only provided a brief glimpse of what happened. Second, some stories were less clearly communicated than others, and it is possible some themes were overlooked, or did not stand out, as the result. Finally, while this data source served the benefit of highlighting the facts which were presumably most important to victims, it also precluded the possibility of conducting a quantitative analysis. Partly as the result of these limitations, the thematic analysis approach used for this study was thought to be best suited for achieving the stated goals. In order to gain even greater insight into the persuasion tactics used by online romance scammers, a quantitative approach, involving a sample of online romance scam victims, would be ideal.

Exposing the psychological techniques used by online romance scammers, and appreciating how powerful they can be, may yield information that can be used to better inform potential victims, and prevent them from becoming ensnared. Of equal importance, this information might also be leveraged to help equip third parties who may be able to intervene in potential scam situations; understanding how scammers obtain compliance from their victims may foster better awareness of the signs associated with online romance scams. Interested third parties might include the friends and family members of potential victims, social workers, members of the financial industry, social media, and law enforcement. It is also hoped that understanding how online romance scammers exploit victims' psychological weaknesses will promote a culture of support for victims, and encourage greater attention to be given to this serious and devastating crime.

References

Anderson, K. (2013). *Consumer fraud in the United States: An FTC survey.* Washington, DC: Federal Trade Commission

Button, M., Lewis, C., & Tapley, J. (2009). *Fraud typologies and victims of fraud: Literature review.* United Kingdom: National Fraud Authority.

Cialdini, R.B. (2007). Influence: The psychology of persuasion. (Rev. ed.). New York, NY: HarperCollins.

Code of Federal Regulations. (2009). §46.102 (f).

Deevy, M., Lucich, S., & Beals, M. (2012). Scams, schemes & swindles. Stanford, CA: The Financial Fraud Research Center.

Federal Trade Commission. (2016). *Consumer Sentinel Network data book for January – December 2015.* Washington, DC.

FINRA Investor Education Foundation. (2013). *Financial fraud and fraud susceptibility in the United States: Research report from a 2012 national survey.* New York, NY: Applied Research & Consulting, LLC.

Internet Crime Complaint Center. (2016). *2015 Internet Crime Report.* Washington, DC: Federal Bureau of Investigation.

Longe, O., & Osofisan, A. (2011). On the origins of advance fee fraud electronic mails: A technical investigation using internet protocol address tracers. *The African Journal of Information Systems, 3*(1), 16-26.

Pak, K. & Shadel, D. (2011). *AARP Foundation national fraud victim study.* Washington, DC: AARP Research & Strategic Analysis.

Ultrascan Advanced Global Investigations. (2014). *Smart people easier to scam: 419 advance*

fee fraud statistics 2013. Amsterdam: Ultrascan AGI.

United States Department of Justice. (2017). “Prince charming” behind bars: Nigerian romance scammer nets 27-year prison sentence. Retrieved from https://www.justice.gov/usao-sdil/pr/prince-charming-behind-bars-nigerian-romance-scammer-nets-27-year-prison-sentence.

Whitty, M.T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Netowrking, 15*(3), 181-183.

Whitty, M.T., & Buchanan, T. (2012). *The psychology of the online dating romance scam.* University of Leicester.

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