Online Romance Scams

A Better Business Bureau Study on How Scammers Use Impersonation, Blackmail and Trickery to Steal from Unsuspecting Daters

BBB International Investigations Initiative
BBB Chicago bbbinfo@chicago.bbb.org
BBB Dallas info@nctx.bbb.org
BBB Omaha info@bbbinc.org
BBB San Francisco info@bbbemail.org
BBB St. Louis bbb@stlouisbbb.org

BBB International Investigations Specialist
C. Steven Baker stbaker@bbbinc.org

Issued: February 2018

Introduction

Singles trying to develop a relationship often turn to an online dating site or app to find someone. A Better Business Bureau (BBB) study was conducted to learn about the inner workings of online romance scams and provide potential targets and reputable dating services with knowledge needed to avoid this widespread and devastating fraud.

The study revealed a massive number of fraudsters are using these sites to gain unsuspecting people's trust to steal their money. The scheme sometimes takes months to build a trusting relationship before the scammer asks for money, usually for an emergency or transportation, from the person they have conned into a relationship.

Victims in the US and Canada have reported losing nearly **$1 billion** over the last three years – and BBB suspects this is only the tip of the iceberg, as most people

do not file complaints with BBB or law enforcement. The emotional harm to victims is even more painful. People who are emotionally shattered by learning that someone they were in love with was a fraudster sometimes even commit suicide.

While some romantic online deceptions are called **catfishing**, BBB makes an important distinction between catfishing and romance scams. In a typical catfishing scheme, the catfisher sets out to deceive his or her victim, but does not at first intend to take money; in a romance scam, the perpetrator intends from the beginning to defraud the victim.

Romance scam victims may be male or female, young or old, straight or gay. The common denominator for victims is that they believe in true love, and they believe they have found it.

One expert estimates that at any one time there may be **25,000 fraudsters online** with victims. One company that screens profiles for dating companies says that **500,000 of the 3.5 million profiles it scans every month are bogus**. BBB estimates that there may be more than a million victims in the U.S. alone, and they may well be people we know. Victims rarely speak out because they are humiliated and embarrassed that they have fallen for a scammer.

The U.S. military says that they have heard from thousands of victims who thought they were dealing with someone in the armed services.

This is a major problem around the world. Much of this fraud comes from Nigerian romance scams, where organized groups engage and support this fraud. The same groups often are engaged in other common types of fraud, and often turn romance scam victims into unknowing accomplices of money laundering. The groups that operate and control much of this activity also may be involved in other types of organized crime, such as prostitution or drug dealing.

Although there have been some significant prosecutions, and the online dating sites are taking some measures to protect their customers, more can, and should be done to stop the fraud, protect businesses' reputations, and provide help for those whose lives have been destroyed.

One scammer's story: Olayinka Sunmola

We begin with a recent criminal prosecution in the U.S. Attorney's Office for the Southern District of Illinois. **Olayinka Ilumsa Sunmola** is a Nigerian citizen who ran this fraud from South Africa. He posted fake profiles on a variety of dating sites using real pictures of actual people, often claiming to be an active officer in the U.S. armed forces. In these profiles, he claimed to be widowed with one child, and to be a practicing Christian with a strong faith.

Sunmola met his victims on dating sites and quickly moved their communication to Yahoo chat, and attempted to explain his slight accent by claiming he was originally born in Italy or Greece. He spent weeks or months developing relationships with his victims, often sending gifts such as flowers or chocolates, and then asked for small sums of money for supposed minor emergencies to test his influence on them. The women often were convinced they had found their true love and soul mate, and often he assured them that they would be married in the near future. In fact, he regularly referred to one victim as "Mrs. Dyess," part of the alias he was using with her.

The **indictment** charges that he defrauded at least 30 women in the U.S. Collectively they sent him tens of thousands of dollars. In addition, he used stolen credit cards to order laptops and iPads, and used his victims as mules to send the merchandise to him in South Africa. Sunmola even had a store selling electronics in South Africa, which operated illegally. Apparently, all of his stock consisted of items he had stolen in one way or another.

Sunmola also had one victim apply for a credit card, get cash advances on it, and then send money to him in South Africa through Western Union and MoneyGram.

Olayinka Sunmola

He promised to pay her back, and at one point did pay off the credit card – with money he had obtained from an online bank account he had hacked into in California. When the bank discovered the losses, they went after his victim for collection. In the end, she filed for bankruptcy as she was left $98,000 in debt.

Sunmola sent four traveler's checks for $1000 each to another victim and again, had her use Western Union and MoneyGram to send the money to him. He claimed to be a military officer traveling on a confidential mission and as such, could not cash the checks himself. However, in the process, the traveler's checks were stolen, and this victim was arrested, strip searched, and faced criminal charges. As a result, she lost her job as a manager at Wal-Mart.

With yet another victim -- who was convinced they were soon to be married -- he had her perform in a sexually explicit manner on Skype, which he secretly recorded. When she refused to send more money – because she had no more to send -- he threatened to post the video online. When she could not come up with more money, he sent a link to these videos to her relatives, claiming he had four more such videos of her and would post them for the world to see unless the "highest bidder" would pay him. Sunmola told this woman by phone that by the time he was finished with her she would want to kill herself. He pledged to ruin her life if she did not continue to send him money. She seriously considered suicide, but survived.

This **BBB study's author, Steve Baker**, witnessed these women testify at trial. They were very brave to appear and take the stand. None of these witnesses seemed unusual and all seemed bright. They had fallen in love, and were willing to do almost anything for the new love of their lives. One of the women even bought a wedding dress and her friends threw her a bridal shower. She went to the airport to meet her "fiancé" and waited all night for him. But he never showed. He later admitted to her that he was a scammer. She said she too considered suicide but changed her mind.

It is hard to know the exact size of Sunmola's enterprise. But we do know that he obtained at least **$1 million in laptops and other stolen electronic gear, and that he obtained at least $730,000 from his victims**.

After two days of a jury trial Sunmola changed his plea to **guilty**, presumably to keep the Court from hearing more details about his activities. At a **sentencing hearing** on August 12, 2016, prosecutors recommended a sentence of 360 months (30 years). **On February 2, 2017 Sunmola was sentenced by the U.S. District Court, East St. Louis, IL to 27 years in prison and ordered to repay $1.7 million to his victims.**

This case was investigated by the U.S. Postal Inspection Service and Homeland Security Investigations of the Department of Homeland Security, and prosecuted by the U.S. Attorney's Office in the Southern District of Illinois.

The South African Police Service cooperated with the prosecutors. They were unable to find any legitimate business in which Sunmola was involved. They seized all four of Sunmola's houses in South Africa, all purchased with cash, as well as the contents of his store. After these assets are liquidated they will be used for restitution to the victims.

"We got great help from law enforcement in both South Africa and the UK," said Nathan Stump, Assistant U S Attorney of the Southern District of Illinois. "Prosecuting an international fraud operation like this one requires tremendous coordination and cooperation among governments, and we were fortunate to have that level of assistance in this case."

How often does romance fraud take place?

Over the last three years U.S. consumers who have filed complaints about romance scams reported losses of nearly $1 billion. The FBI's Internet Fraud Complaint Center (IC3) estimates that romance fraud causes the greatest dollar loss of any fraud or scam that affects individuals, with the exception of investment frauds. The number of complaints, the large money losses, the number of fake profiles, and other data illustrate that this is a massive worldwide problem.

Romance scams in the United Kingdom

One organized effort to gauge the extent of this fraud has been undertaken in the U.K. Professor Monica Whitty undertook a phone survey of the U.K., and in 2012, published a **study** concluding that since this type of fraud began (since roughly 2008) there had been **230,000 victims of this type of fraud just in the UK**. Additionally, she found that 1.1 million people personally knew someone who had been a victim of online romance fraud. Given that the U.K. has one fifth the population of the U.S., this suggests that there are more than 1 million romance fraud victims in the U.S. No similar studies have yet been conducted in the United States.

Complaints

Complaint numbers, while useful, do not provide a reliable guide to the true scope of the online romance scam epidemic. Victims may not even know they are fraud victims for some time, and when they do find out, they are so devastated that they never file a formal complaint, or do not know where to go to file a complaint, so these stories do not become part of a national database. Furthermore, FTC studies show that less than 10% of all fraud victims report it to BBB or law enforcement.

BBB regularly receives reports of romance type fraud via its Scam Tracker system or when filing complaints about being scammed when using services of online dating companies. Complaints are then downloaded into the Federal Trade Commission's Consumer Sentinel database, which includes not only complaints made directly to the FTC but includes complaints from sources such as Western Union, the US Postal Inspection Service, some State Attorneys General offices, and other organizations. The FBI's Internet Crime Complaint Center also receives large numbers of complaints.

	2015		2016		2017		
IC3	12,509	$204M	14,546	$220M	15,342	$263M	
FTC	8,715	$33.5M	11,149	$75.1M	16,937	$88.4M	
TOTALS	21,224	$237.5M	25,695	$295.1M	32,279	$351.4M	**$884M**

Canadians also are often victims. Here is victim data from the Canadian Antifraud Centre:

	Complaint Totals	Dollar Losses
2015	1571	$16.8M
2016	1921	$18M
2017	1776	$17.6M
TOTALS	**5268**	**$52.4M**

Demographics of victims

IC3 found that for those who reported their age, over half were over 50 years old, and they accounted for 70% of the total losses.

Canada reports that they get twice as many complaints from females than men, with the majority of complainants falling between the ages of 50-60 years old. Over half of the complainants fall in to the 40-70 year old age range.

Also, a 2017 BBB Risk Index report issued by Council of BBBs found, by analyzing BBB's Scam Tracker data, males between the ages of 45 to 54 are most susceptible to the romance scam. The median loss was $2,373 and they tend to send money via website wire transfer. The susceptibility percentage was 48.5%.

Other countries affected

In addition to Canada, **the UK**, and Australia, romance fraud has been reported as a problem in **Hong Kong**, **Malaysia**, **New Zealand**, **Korea**, and **Israel**.

What effect does this have on victims?

The most obvious result of this fraud is the substantial loss of money. There are regular reports in the media of victims losing thousands of dollars. Often victims do not just send their own money, but they also borrow from friends and family members, max out their credit cards, and even cash out IRA's consisting of their retirement savings.

When the victims finally realize that they have been defrauded they often are emotionally devastated, not only due to the theft of money but to the betrayal of what they believed to be an 'intimate' or 'true love' relationship. According to Australian law enforcement officials, while unconfirmed, they believe that there are more suicides in Australia due to romance scams than there are murders. The operator of a support group for online dating scam victims says that every member has contemplated suicide.

Even victims that do not lose money may face serious emotional issues when their "relationships" end. Victims who lose all their money are in desperate financial and emotional straits. Some require public assistance once their money is gone.

Anatomy of a romance scam

Professor Monica Whitty in the UK has **studied the psychology of romance frauds** and found that they develop through several distinct stages. First, devising an online profile and making contact with vulnerable victims. Second, developing a trusting relationship by isolating and grooming the victim, learning as much about the victim's family, background, dreams, and assets as possible. Many of these tactics are similar to those used by predators of human trafficking and online child pornography. Third, they find a way to get the target's money. During this process, they also may use these victims as money mules to process money for other frauds. Finally, many times the same people are re-victimized after they learn they have been defrauded. Let's take a closer look at each step.

How do they contact victims?

The romance scammers operate on dating websites, but sometimes use Facebook and other social media. Some romance scam activity takes place on Google Hangouts. Obviously, scammers focus their efforts on those most likely to be interested in the "relationships" they offer.

There are hundreds of dating websites and apps operating around the world with familiar big names like **Match.com** and **eHarmony,** two of the largest worldwide. Some of these online dating services charge a monthly fee to access their services. Others, such as **Plenty Of Fish**, are free. There also are

sites tailored to different religious or ethnic groups or for people with other commonalities, such as **farmersonlydating.com** or LGBT sites.

Because the scammers are, after all, crooks, many of them use stolen credit cards to join sites and post fake profiles. In this situation, they try to meet victims, interact with them, and quickly move them to a different form of communication, such as email or text messaging. Thus, when the dating company notices that the credit card information is bogus, and removes the profile from the site, the fraudster can continue to stay in contact with the victim.

The dating sites try to keep the frauds off of their sites as it affects them negatively as well. When these sites have bad credit cards submitted this affects their relationship with the credit card companies, and may increase the dating companies' costs for credit card processing. The free dating sites cover their costs by advertising, and have some incentives to ensure that this advertising is viewed by people who may actually be potential purchasers.

At the site the fraudster sets up a profile, complete with a picture and information about the person they're posing to be. As noted, convicted fraudster Sunmola often pretended to be with the U.S. military. Pictures often are simply copied from other locations on the internet. These pictures are important to the victims as they are developing their mental image of the person with whom they become emotionally involved.

Fraudsters often make up fake Facebook pages for their aliases as well. This paints a picture of plausibility that helps the victim believe that they are dealing with the person represented in the profile.

Who do they pretend to be?

Those engaging in online romance frauds try to build personas of people that they think would best attract the opposite sex. For women, they typically claim to be men that are financially stable, such as business owners or professionals that work internationally. Sunmola's profiles also regularly claimed to be a widowed father of a minor child. Bringing the child into the equation seems designed to speak to the maternal instinct in victims, as well as to establish that the scammer is a responsible parent and, thus, presumably a solid potential partner in life. Having a supposed child can provide the pretext for emergency requests for funds. It is also common for the profiles used to claim a strong religious faith, denoting someone with strong values and, thus, solid and trustworthy.

In Whitty's **2012 *CyberPsychology, Behavior, and Social Networking* article**, she finds that profiles targeting male victims tend to feature attractive young women, under 30 years old, who are financially dependent and need someone to help them, such as a nurse, teacher, student, or the owner of a small business. They describe themselves as honest or trustworthy. Again, they steal photographs from other websites. And, they feature attractive young women and use the lure of sex. They rarely portray themselves as living in Africa.

The study found that profiles aimed at gay men featured photos of attractive young men, no older than 40, with a mix status of semi-professional jobs or successful businessmen. They often claim to be in the military. Again, these profiles rarely portray themselves as being from Nigeria or Ghana.

Use of the Military

It is common for profiles to claim to be for people in the U.S. military, and this approach is used all over the world. Sunmola, for example, concentrated on women, typically those recently widowed or divorced, and often over 50. He often used the name and picture of a Colonel in the U.S. Army stationed overseas.

Chris Grey is head of public affairs for the **U.S. Criminal Investigation Command.** He says that they get thousands of complaints from romance scam victims around the world. His unit also works with U.S. Embassies around the world, who themselves hear from victims. He says that the frauds have used photos of soldiers killed in action in Afghanistan or Iraq, and they have even used the photo of the Army Chief of Staff. At times the victims locate the real person in the military, who are understandably upset with their photos being used to defraud people. In at least one case, a soldier's wife learned of the profiles using her husband's picture and she thought he might be cheating on her (he wasn't).

The frauds also use pictures of women in the military. Because members of the armed services aren't themselves being defrauded there is little they can do to take action against the frauds, though he says on a few occasions they have been able to have photos removed from social media. He reports he is frustrated that there isn't more he can do for victims.

CID has a web page giving warning tips and examples of bogus documents used in the fraud. For example, military people will never need money from romance victims for leave or healthcare. He also advises that everyone in the military will have a ".mil" email address, and to ask supposed soldiers to send an email from that address. His group has also set up **a facebook page** to help with this problem. The Marine Corps also have been making **efforts to tackle romance frauds using social media**. Here is an **interview with one man in the U.S. Army** that learned his picture was being used for fraud.

The Grooming Stage

Once initial contact with a victim has been made, the "relationship" continues with a grooming phase, in which the fraudster learns about the victim's life and builds trust. Because the frauds are a business for the crooks, it is not surprising that they use the same profile language,

pictures, and standard emails for a number of victims.

Here is a **set of scripts** used by romance frauds that show the progression of emails used over time.

There also are situations where the victim receives a text message when they wake up every morning professing everlasting love. Some scammers even send flowers or other small gifts to their victims. They may text the victim 20 times a day, mirroring what everyone would want their 'true love' to share. The scammers also may request small favors in return, which allows them to gauge whether the victim is likely to be susceptible to the inevitable time when there is an "emergency" requiring that the victim send a substantial sum of money.

These interactions build trust. Remember, 'con man' is short for confidence man, a person whose expertise is gaining your confidence. We trust other people every day. If we go to a doctor people rarely check with a medical school to ensure the doctor is not an imposter. Or if someone pulls up behind our car with flashing lights we of course presume that they are actual police and not an imposter. We reasonably rely on quick indicia of reliability to make quick decisions – was he or she wearing a badge? Did it look like a police car? These types of indicia can be employed by frauds to provide some background information that help foster belief.

And we often think that only dumb people would fall for something like this, and that with use of their own common sense and skills, they would be able to detect a fraud. The simple truth, however, is that the crooks are very skilled professionals, and it is often very difficult to detect a fraud relying only on our own snap judgments.

The grooming process also focuses heavily on isolating the victim from their friends and families. When victims report concerns by others in their lives, the fraudster often urges the victim to question the motives of other people.

Another reason that the fraud works is that the fraudsters tell us what we want to believe.

The grooming process may take a few weeks or as long as a year, moving on only when the fraud concludes that the victim is attached and ripe for parting with money.

The sting

At some point the fraudsters will want money, usually for a medical emergency, a business problem, or to pay for a plane ticket to fly and meet in person. If the victim complies, the romance scam will continue on a variety of pretexts to keep the victim sending more money. These can be quite elaborate stories, at times involving supposed third parties. For example, some victims were told that funds necessary for the supposed businessman to continue operating had been sent from the UK to Ghana, but $3000 or more was needed to renew diplomatic seals on the funds so that it could be released.

It is not uncommon for the frauds to employ bogus web sites as part of their schemes. These can include banks or courier companies to handle the transfer of money that the fraudster needs to have for business purposes. There are also a variety of fake government forms meant to prove the fraud.

Some of these frauds also claim that a package or present has been sent to the victim. Then the victim hears from a supposed third party, such as a Customs agent from another country, telling them that there is money that must be paid before the present can be delivered. If the victim pays then there may be a parade of additional monetary demands as the package supposedly works its way throughout the world.

There have been times when victims were encouraged to fly overseas to meet their love interest. Professor Whitty found that some of these victims were kidnapped when they flew to Ghana to meet their supposed soul

Grooming Scripts

Some scammers reuse successful scripts to trick their victims. This script was used toward the end of a scam.

Darling, I have been trying to reach you on phone but I guess network has been a jerk. I am just coming back from the South Africa tax office, Johannesburg with the customs officer who is to find out about my tax payment on the equipments. Last night while I was already in the plane and my and equipments were till under check, just when the flight was about to get ready for us to take off. A custom man came in and called my name, they asked of my tax clearance on the equipments since I told them I used the equipments in their country working on a building project for over one year (14 Months).

They wanted to call the tax office same time to verify if I am good to go but they were closed so they delayed me till this morning and promised that I would fly on the next flight. Right now, we just got back from the tax office where I was checked and billed. They said during the course of such a big project, I ought to be paying R8,961.91 ($1,099.00 USD) which is about R116,504.83 ($14,287.00) for thirteen months. The tax office is not a body I can negotiate with so I didn't even try to tell them I will pay them once I clear my check because I don't want any one else to know I have a check of such a huge amount.

I am at the airport now thinking of moving back to the hotel room and explain things to them if they would allow me stay for the time being. I have my luggage but I don't know if they would release my equipments to me. I asked if I could leave the equipments and then come back for it, they said that is not an option, the worst of it is that each day my equipments stays at the airport, I pay additional R350 ($42.7602 USD).

I am perplexed right now! I feel like I'm in a very wrong country!! I don't know what to do!!! I shed tears but it won't put me on the plane so I stopped. We have few hours to get together and this kind of thing is happening, dear, please call me, I need your sweet voice to calm down my heart before I develop high blood pressure. I want you to forget about this tax bill for now, let us put our minds off it and first get myself into the hotel room to have some hours sleep. It's been a long day full of stress.

Maybe when I wake up we can then talk and think of what to do. For now, I don't want us to think of this because the rate at which it hurts could lead us into another bad situation. I just don't want any of us to die of these stress because we still need each other for many more years. I love you so!

Your Husband,
Ben.

mates. They were shown money sent in their names, and then were locked in houses for several days. Men with firearms appeared, had the victims sign forms attesting that their money was not for drugs, and then finally sent them home.

The fraud continues

If the victim has realized that they have been defrauded, the fraud does not necessarily end. Victims may be contacted by someone impersonating a law enforcement agency or government agency that wants to help them recover their 'lost' funds. The victims Professor Whitty interviewed reported getting emails supposedly from law enforcement in West Africa claiming that the scammer had been caught, and their money could be returned if they spend several thousand dollars for the fees needed to release and return the money.

It is not uncommon for the scammer to contact victims again, admit that it was a scam, but claim that they actually did fall in love with them. Victims that stay in contact are at risk of losing additional money or becoming involved in assisting the fraudster in other scams.

Victims often continue on dating sites looking for a relationship and may again become involved in an additional online dating scam. Fraudsters also sell lists of victims to other fraudsters.

How do scammers get the money?

There is no point in running a fraud unless you can get money. Companies like Western Union and MoneyGram are the payment method of choice. Sunmola, for example received a great deal of money sent to him through Western Union in South Africa. However, in some types of fraud the crooks may use bank to bank wire transfers.

Western Union is the largest money transfer company in the world, with agents in almost every country. Some scammers prefer to use MoneyGram, since virtually every Wal-Mart in the U.S. offers MoneyGram services.

In order to send money through either company a consumer must take cash in person to the agent and complete a "send form" which includes the sender's name and address. *(There are situations where you can use a credit card to send, but scammers rarely want victims to employ that form of payment since consumers can later dispute the charges).* These forms also designate who is to receive the money and where.

It is important to know that money does not have to be picked up at the address specified. While both Western Union and MoneyGram have amended their practices somewhat in recent years, traditionally it was possible to pick up the money anywhere in the designated state or province or in any contiguous state. So, victims will not know where the money was actually released.

Those receiving the money must complete a "receive form," which requires the agent paying out the money to record the ID presented in the company's database. So Western Union and MoneyGram should have records for all sends and receives available in their central computers.

In Nigeria, one can only collect money from Western Union or MoneyGram at a bank where the receiver has a bank account. Although this should control some of the fraud, in reality, people can use fake ID's to open bank accounts, and bank employees may themselves be either corrupt or complicit. In Spain, recipients had to produce a passport to receive money. Agents were recording passports with pictures of people like Angela Merkel, Cameron Diaz and Sandra Bullock. The Spanish National Police brought charges against nearly 200 Western Union agents. No one actually came in to the agent location to pick up the money. It was just collected by the agents and often simply re-sent to Nigeria.

In January of 2017 Western Union settled civil and criminal charges with the **Justice Department** and the **Federal Trade Commission**, agreeing to improve anti-fraud efforts and to pay $586 million to victims. The **FTC settled with MoneyGram** in 2009 for similar conduct.

Both MoneyGram and Western Union have fraud controls in place. The typical remittance to a family member (the principal legal purpose for using these services) is only a couple hundred dollars. Transactions of $1000 or more stand out and may be screened by the companies. As a result, the scammers tend to have victims send more transfers for lesser individual sums.

In addition, MoneyGram and Western Union have programs in place in which a victim's name can be provided to their fraud departments, and these money transmitters can actually block the victim from sending (or receiving) additional funds. These companies now also share these lists with one another.

It is a good program for law enforcement, Adult Protective Services and family members to be aware of as a resource. Contact both companies' fraud departments for more information on this option. But be aware -- scammers may simply instruct the victim to use a fake name as a loophole.

The fraudsters also may attempt to use other payment methods, such as bank to bank wire transfers. However, under the anti-money laundering laws, banks are on the lookout for these types of methods of using money, and must complete a currency transaction report, or CTR, for transfers over $10,000. Moreover, there can be a paper trail. However, this is an increasingly popular method, especially if the victim also is being used as a money mule. In addition, the banks will be wiring the money to overseas banks, where stopping the funds may be more difficult. This method of transferring money is used at times, but it explains why the fraudsters prefer to instead use the money transfer companies. If a victim is involved in this, report it to the bank and IC3.gov immediately to request a stop on the account's funds being moved, pending further bank/law enforcement investigation.

What do we know about victims and why they fall for this?

Perhaps the initial reaction of most people hearing about this fraud is to presume that the victims are simply

gullible (because we believe we would not ourselves be taken). Some believe that this fraud affects primarily late middle age women who are, by implication, desperate or depressed and therefore vulnerable, when in fact, the studies suggest that this is not necessarily the case. It is an important question, since educational efforts in intervention and prevention must be crafted to the correct audience if they are to be effective. Needless to say, knowing who we are dealing with their motivation is important for knowing how to help victims later.

Whitty has done some of this work in a **study** involving interviews of romance fraud victims. She surveyed victims and asked if they were men or women, rich or poor, straight or gay, older or younger. Surprisingly, she found no correlation in any of these categories. Instead, she noted two consistencies: individuals higher on romantic beliefs were more likely to be victims of the romance scam, and participants with a higher tendency towards the idealization of romantic partners were more at risk of being scammed.

This type of fraud can and does affect men as well as women, younger as well as those older, and gays and lesbians as well as heterosexuals. The one thing victims had in common was a strong belief in true love and the existence of a soul mate ... and they believed that they had found that.

(Note that this does not necessarily mean that different groups of consumers report this fraud at the same rate.)

Real-life stories reported to BBB

A California woman, Ann, lost $22,000 to a romance scam and is now totally broke, in debt to her credit cards, and living with her daughter.

A year after her husband died, Ann decided to try online dating on Match.com. Before long she heard from a man who called himself "Wayne King." They began communicating, first through Match.com and then over text.

King claimed to own a company called Jev Orbital in Maryland, and with an internet search she found this company really did exist. King claimed to be 66 years old, and said he lived in Pasadena. When she asked he even provided the address. He said he had a daughter in Baltimore, Maryland. He tried to gain Ann's confidence by showing her information that he said showed she could access his bank account, which contained more than one million dollars.

Photo was used by the scammer to deceive Ann (face blurred)

When King said his daughter was in the hospital Ann sent some money to help. Then King said he was in Beijing, but was having trouble shipping goods for his business to the U.S. He asked Ann to help him to pay to ship the goods through Malaysia to the U.S. Over the course of a month Ann sent King $22,000 on the strength of his promises to pay her back. After Ann agreed to pay for the shipping fees, King asked her to buy him four iPhones and a Macbook Pro. She maxed out her credit cards to buy these and ship them to him, again on the promise that King would pay her back. He never did.

At 69 years old she is now taking pills for anxiety, may need heart surgery, and is filing for bankruptcy. Her daughters told her she needed to report this, and Ann went to the police and also reported it to the Better Business Bureau. Despite the heartache she has suffered she agreed to share her story to help keep others from suffering through a similar experience.

A Pennsylvania woman, Josie, was contacted on Facebook by a man calling himself "Mark Richardson. They messaged each other, and eventually she gave him her phone number. They began sending flirty texts. He told her that his wife had died of cancer, and that he had a 9 year old daughter. He told her he loved her, and they would form a perfect family.

Photo sent to Josie by the scammer (face blurred)

Richardson wouldn't let Josie visit him, but said he wanted to visit her, and asked for money to buy a ticket. Several months later he told her he had a great surprise – he was going to buy a house in her town. He wanted her to get involved with the deposit on the house, but she refused.

Richardson began to ask for more money for his expenses. Josie sent him money for a new phone and for a car payment he said he couldn't afford. He wanted more money, and later her credit card number, but she refused. He got angry, and she became suspicious and cut off communication.

When Richardson contacted her again, he said he was in Canada and was using a new name. Josie told him she knew he was a scammer. At this point he told her that she was too smart for him. He said he really was a scammer, that he was an engineering student in Nigeria and that this is how he paid for school. He said though they met as a scam he really had fallen in love with her. Josie once again ended communications and reported the scam to BBB.

A woman from Colorado, Hope, was using the dating site OK Cupid when she was contacted by "Paul Dreyer." Paul said he was an engineer working overseas on a contract. He said his wife and parents were dead, but that he had a young daughter who was living with his family, and that they had a house in St. Louis. Hope mainly communicated with him by text or email, but did talk on the phone once or twice. He had an accent, but he said he was Italian and originally from the east coast.

They communicated for some time, and he was quite flattering. Paul said he would be home in 2 to 4 months and they would then meet in person.

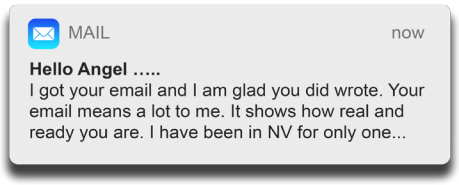
Paul then said he needed to borrow some money to help with his daughter's school. He asked Hope to wire him $350 and also to buy $250 in gift cards.

Hope talked to her mother and stepfather about the situation, and they helped convince her that something was not right. She was able to stop the wire transfer, and had taken photos of the numbers on the back of the gift cards. She was able to cancel the cards and got all but $76 of her money back.

Paul kept harassing her, even calling her at work. She finally told him off, cut off contact with him, and called BBB to report the scam.

Hope has since been contacted by several other men, including one who said he was in the military in Libya. She decided he was probably a fraud and she blocked him.

Hope urges people to be very careful when meeting people online, especially if they say they are overseas and cannot meet in person.



Who is behind this?

The vast majority of romance fraud has its home in West Africa, particularly Nigeria. In fact, cybersecurity expert Lawrence Baldwin of Mynetwatchman says that at any given time, there may be more than 25,000 romance scammers online with victims, with the vast majority of them coming from Lagos, Nigeria.

It is not clear why Nigeria is the source of so much fraud, though it is the largest country in Africa. It is also a former British Colony, so most Nigerians tend to learn English. And it has an educated population, but there is high unemployment. Over the last few decades there has been a diaspora of Nigerians who have moved across the world. Thus, there are large native Nigerian populations in South Africa, Canada, the U.S., Malaysia, China and many other places.

Nigerians are not alone in dating and romance fraud. Scamsurvivors.com, a volunteer group that has battled online romance fraud and helped victims for many years, says that there also are separate groups in Russia and the Ukraine that employ online dating sites to defraud victims. Members of the group report that often, Russian scammers ask for money to cover the expenses to visit the victim in their country, while Ukrainian scammers ask for money to pay a translation agency to continue translating their emails as they don't speak English well. The group suggests that Russian criminal gangs concentrate on single men, urging them to visit Russia to meet a potential bride. If they do, they are accompanied on their "date" by an interpreter that serves as an enforcer. The victims are encouraged to spend large amounts of money on an apartment, a translator, presents, lavish dinners, and other expenses. But they do not get married, and are never alone with the woman. Some victims are beaten and robbed. It is also very common for this type of fraud to target gay men.

Those engaging in these frauds do not necessarily limit themselves to one kind of fraud. Sunmola, for example, made more money from buying electronic goods with stolen credit card numbers than he did from his romance fraud victims. Nigerian criminals operate not only online dating scams, but often engage in house or apartment rental frauds, Business Email Compromise Fraud, filing bogus tax returns, running frauds that employ counterfeit checks, buying goods with stolen credit card numbers, and a variety of other frauds.

The Nigerian frauds tend to operate in cells of 10-12 people, with a leader called an "Oga" to organize efforts. Young men at the lower rungs of this system are known as Yahoo Boys, and they may begin simply sending initial contacts to thousands of people with profiles on dating sites or who are on social media. Only a small percent of those contacted will reply, and further contacts are then passed along to more senior members of the group to take charge.

There also is very clearly a worldwide network of those engaging in fraud. There are groups that develop fake dating site profiles and others that develop scripts for the text messages and emails used in romance scams. In 2016 a woman in the UK that wrote scripts for romance scams was convicted of fraud and **sentenced to two years in jail**.

In addition, there are people who develop fake websites and documents used to lend an air of legitimacy to the frauds.

The fraudsters even hire experts who help polish up prose and grammar in messages. And, there are money moving mechanisms around the globe.

In short, this is organized crime on a worldwide scale. **Work done by Canadian law enforcement** demonstrates that members of the Black Axe Nigerian crime syndicate engaged in controlling and organizing fraud activities throughout the U.S. and Canada.

Romance scam victims used as mules for other fraud

So, what does a romance scam operator do with a victim who has no money to send or who has already sent their money? These people are still a very valuable resource because they can be used to launder money from other victims by acting as money mules. In the last couple of years law enforcement has come to recognize that there is a very large group of money mules that

receive money, or goods purchased with stolen credit cards, and then send that out of the U.S. Romance scam victims could then be aiding and abetting other types of frauds. The use of these "mules" makes it much harder for enforcers to recognize the scope of fraud or to identify the perpetrators and take action.

Terrill Caplan of Fraud Aid has spent years working with, and often helping romance fraud victims who have been employed as money mules. He estimates that there are at least thousands of dating site scam victims in the U.S. that are being used as money mules. He estimates that less than 20% of romance victims are used as mules, but this is still a large number. He says most victims do not realize that they are helping illegal activity and stop the conduct when they learn that it is illegal.

There is little reason to think that romance scammers limit their fraud activities to operating romance scams. There are a wide variety of frauds that operate out of Nigeria and West Africa. Most of us probably instantly think of the ubiquitous emails claiming that the consumer is the beneficiary of an inheritance from a dead dictator or the like. But while the number of complaints about those letters (or emails) have been declining for several years, this is still a crime that steals life savings from thousands of people every year.

For example, in November 2017 a **67 year old man was arrested in Slidell, Louisiana** and charged with handling over $250,000 in money from victims around the country that came from romance and Nigerian prince frauds. He is facing 269 counts of wire and mail fraud. He apparently began as a victim, and but later started working with the frauds, taking a share of the proceeds himself before sending funds to the fraudsters.

Use of online romance scam victims as mules is common in Business Email Compromise (BEC) scams, in which the fraudsters trick businesses into doing bank to bank wire transfers into an account opened by a mule/victim. According to IC3 these BEC crimes produce the largest losses of any of the crimes they track.

The U.S. Attorney's office in the Southern District of Mississippi has had great success with Operation Scams R Us, which **indicted 20 Nigerians** living in Nigeria, South Africa, the U.S., and Canada. This began with a romance fraud, in which a victim had received a package that she was instructed to send along to South Africa. The Defendants used romance fraud victims to help them with counterfeit check frauds, reship electronic goods purchased with stolen credit cards, send money on to Africa, and with other frauds. Three Nigerians that had been extradited from South Africa were **sentenced** after a jury trial in Mississippi and received 115 years, 95 years, and 25 years in prison.

Romance scam victims are good vehicles for laundering the money for fraud. Scammers build a trust relationship with their victims, and isolate them from other's advice. So, there is little risk that the romance scam victim will pilfer the funds or goods they receive. Moreover, unlike a co-conspirator or agent in the U.S., these victims are less likely to ask for pay to perform these services. And even if law enforcement locate and confront the romance scam victim about their money laundering efforts, the victim does not know the true identity and location of the person they are really dealing with and therefore, cannot provide that information to law enforcement. In addition, the scammers realize that most local law enforcement is unlikely to follow up on a fraud complaint and follow the money to the mule/victim because the money has gone to somewhere in the U.S. that is out of their jurisdiction.

In addition, some romance scam victims have been used to transport drugs – and have been imprisoned. In most cases, the victim was involved in a lottery or romance fraud, and was convinced by the scammer to travel with a suitcase or other item, which they did not know contained drugs. The Internet Crime Complaint Center estimates that 144 elderly couriers have been conned into (unwittingly) carrying drugs overseas. Over 30 such people have been incarcerated. In February 2016, **the Senate Aging Committee held hearings** on precisely this subject.

And on July 29, 2016 there was a report that a 77 year old minister from Maine, who was a romance scam victim, **was released from prison in Spain**. He had originally been sentenced to six years in a Spanish prison for transporting drugs.

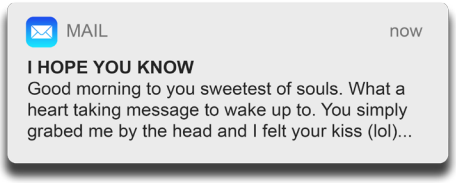
An Australian grandmother had been asked by a romance scammer claiming to be in the U.S. Special Forces to travel to Shanghai, pick up a package for him, and carry it back to Australia. When she went through Customs in Malaysia, they found methamphetamines in the lining of the bag. She was arrested for drug trafficking, a crime that carries the death penalty. After a trial, she was **acquitted in December 2017**.

How can you tell if someone is dealing with a fraud?

Obviously, the general rule must be that if you meet anyone online, and for some reason cannot meet in person and requests money, there is a very high probability that it is a fraud. Do not loan or give personal identifying and financial information or send money to someone in an online romance or over the phone.

Engaging with the scammer to test their credibility is unlikely to work because they do this every day, they know how to respond, and pressing them may lead them to threaten to terminate the relationship and end the torrent of positive feedback they have been providing their victim.

It is very difficult to dissuade a romance scam victim from continuing. This type of intervention also takes a very thought out and sensitive process, with follow up victim services, counseling (by trained mental health providers), advocacy services, information on reporting, financial counseling, possible creditor intervention, access to support groups (both online and local).



Victims will often need information on available benefits, housing refinancing or assistance programs, and possibly bankruptcy information.

Here are some tools that could help convince a victim that they are not dealing with the person they think they are.

Quiz ScamSurvivors.com has provided an **online quiz** to help determine whether an online romance is a scam.

Check the photograph The initial profiles that the scammers post will almost always have a photograph. Victims usually keep these, since they have not yet met the person. There are search engines that can fairly reliably search pictures like **Tin Eye**. Google Chrome also allows you to put the cursor on a photo, right click, and search the picture. If the same picture appears with other names and in other places, this is the best possible method of detecting a fraudulent profile. (*Of course the frauds have methods of making this search fruitless, such as reversing the picture which makes it more difficult to search).*

Search the text In addition, an internet search of an unusual twist of phrase from a profile or email may turn up posts showing it was used in a different romance scam. Because scammers are dealing with so many victims, they will inevitably use the same language for other victims. You could even try searching for a paragraph of text.

Use the State Department to transfer funds for an emergency Fraudsters often pretend to be a U.S. citizen working overseas or a member of the armed services. The State Department often hears of such frauds. They try to provide help to U.S. citizens suffering a real medical or other emergency. On their **website** they note: "If you insist on sending money to someone who claims to be a U.S. citizen, consider sending money via the Department of State's **OCS Trust**, which requires the recipient to show a photo ID to collect the money." Call the State Department's Office of Overseas Citizens Services at 1-888-407-4747.

Check to see if there is a real business overseas If the fraudster claims to own or be working for a business overseas call the U.S. Embassy in the appropriate country and they will verify if this is a real business and provide some background on the company.

Check to see if someone in the military really needs money. Fraudsters impersonating the U.S. Military often claim that there is some reason that the military can't provide needed funds – and that thus the victim needs to help them. This **website explains how this works**, and provides examples of fake government forms that the fraudsters commonly use. .

It is possible that if victims knew how the scam works, and how prevalent it is, they might recognize that they are involved in the same activity. Showing them warnings and other articles about romance scams could help.

What can dating companies do?

If the bogus profiles on dating and social media sites were removed, this would severely limit the ability of the frauds to contact potential victims.

There are businesses that work for dating companies to try to keep these profiles off the sites. Dave Wiseman is Vice President of Sales and Marketing of Scamalytics, a company that collects dating profiles and screens them on behalf of a variety of online dating sites. He says that Scamalytics checks around 3.5 million dating profiles every month and identifies at least 500,000 as scammers (over 15%). Most are identified within 10 seconds, allowing the dating sites using the Scamalytics network to stop them from ever contacting real users. Here is their **2015 report on trends and tactics of online dating scams**.

There are other efforts underway to screen the profiles and prevent fraud. Giancarlo Stingili is an associate professor at University College in London who has been studying the profiles employed in romance frauds as part of a larger project on detecting and preventing mass marketing fraud. He believes that there are organized crime groups that specialize in developing profiles that online dating scammers can use in their efforts to attract victims. Studying the characteristics of these profiles can, he hopes, help in educational efforts.

He notes that many of the profile pictures show the "person" in a group shot, suggesting to victims that they are outgoing people. He says the frauds may Photoshop faces onto stock photos, and that they remove metadata that can sometime be used to learn where and when a picture was actually taken.

Giancarlo is using this study to try and develop a program employing artificial intelligence to identify profiles used in romance fraud. He hopes that an algorithm he is developing can help to identify fraud profiles, and that with AI, it can learn more characteristics and improve its own fraud detection abilities.

The online dating companies need to use their best efforts to keep the crooks off of their sites. If nothing else, it would seem that they should be able to note the use of clients using IP addresses from Nigeria or other suspect locations that do not match the profile.

Another recommendation is to warn their customers that this is a problem. Some of the dating companies do have warnings about romance scams, but these can be difficult to locate on the dating websites and are somewhat generic. Consumers seeing these might not recognize that this is a common and serious risk. More can be done.

FTC staff and the State Attorneys General have suggested to online dating companies that when they find a fake profile they should directly contact everyone that has been in contact with that profile and warn them of the serious risks and to exercise special care. An association of dating companies in the UK has agreed to take these steps.

Finally, online dating companies could take efforts to help consumers that have been defrauded on their sites. At a minimum, they can take consumer complaints or direct victims of online dating scams to law enforcement and BBB. They also could fund efforts to help defrauded consumers.

Prosecutions

Those running these frauds deserve to be behind bars. Unfortunately, there have not been enough prosecutions. Many law enforcement agencies tend to begin investigations based on a single victim, and may not recognize the true scope of the crime or that there are many other victims. Additionally, where the perpetrator is not in the U.S., many prosecutors are unwilling to undertake the considerable time and expense of locating and extraditing someone.

However, the EFCC in Nigeria has agents and an affirmative desire to work with law enforcement agencies. They also have, themselves, conducted some prosecutions. For those who have an interest, it would be useful for them to talk through how to investigate and prosecute with another agency that has done one of these cases.

Law enforcers investigating this fraud know that the fraudsters have a challenge in keeping the details straight when dealing with many victims at the same time and remembering their individual details. These frauds use some system of records or files to keep tabs on their victims, and whether those are stored on paper, in an email account, or on some other electronic form, they most likely exist.

Where to complain – and why

Many victims are very reluctant to file a complaint. Filing a complaint, however, may help prevent someone else from being defrauded because most fraudsters have many victims. As noted, Sunmola was dealing with at least 30 women. Victims should report these crimes to their police department, IC3.gov, FTC.gov, FBI, Department of Homeland Security, and BBB. Also, report fraud to any internet dating sites in which they 'met' their scammer. And report to Western Union, MoneyGram, their banks and any other financial accounts used.

Resources

U.S. Law Enforcement

Federal Trade Commission (FTC) or call 877-FTC-Help. FTC database of fraud complaints is available to over 3000 law enforcement agencies. Because it contains personal information on fraud victims, it is not available to the general public. It can be easily searched, and could locate victims defrauded by the same person.

Internet Crime Complaint Center (IC3). FBI's IC3 takes the majority of law enforcement complaints about romance fraud.

Scam Survivors is an organization that helps romance fraud victims from around the world, with useful resources and a forum for survivors.

Better Business Bureau takes **fraud reports through the Scam Tracker program**. This also shows the types of fraud reported in your particular area.

Senate Subcommittee on Aging Fraud hotline

Western Union 1-800-448-1492

MoneyGram 1-800-926-9400

Canadian Law Enforcement In Canada, contact the **Canadian Anti-Fraud Center**. 1-888-495-8501

There are local resources for citizens of **The UK**, **Australia**, **Nigeria**, and the **Netherlands**.

Help for victims

Romance scam victims often suffer emotional pain that is at least as serious as the loss of money. As noted, this can and does result in suicides. Often the fraudster has worked hard to isolate the victim from their family and friends – their normal support networks. Those who work with these victims says that the trauma is very similar to that suffered by victims of domestic abuse.

Unfortunately, there is no single place in the U.S. or Canada where victims can go for counseling or similar help, and many doctors, counselors and other care givers are not familiar with romance frauds or how to address them.

If doctors encounter victims they can authorize counseling. If victims are seniors they may be able to obtain help through Adult Protective Services, which has offices in every state and many counties. **Find your local office here.**

Recommendations

More intelligence Although there have been some excellent prosecutions, enforcement agencies should share information from those successes, do more training, and encourage more prosecutions.

Screening profiles BBB recommends that online dating sites and social media do more to screen, identify, and remove profiles used for catfish scams.

Support services for romance fraud victims Because romance frauds often have a serious emotional effect on victims, more support groups should be formed to assist victims.

About the Author Steve Baker is the former Director of the FTC's Midwest Region where he worked on consumer fraud matters for more than 30 years. He serves on the Board of Directors for the Council of Better Business Bureaus and is BBB's International Investigations Specialist.

Previous BBB studies include **Puppy Scams** *How Fake Online Pet Sellers Steal from Unsuspecting Pet Buyers* and **Pop-Ups and Imposters** *A Better Business Bureau Study of the Growing Worldwide Problem of Computer Tech Support Scams*.