

# The Dot-con

---

**Research Project for Emerging Issues/Advanced Topics Course**

**Diploma in Investigative and Forensic Accounting Program**

**University of Toronto**

**Prepared by Un Chi Kuan**

**6/20/2015**

**For Prof. Leonard Brooks**

## Table of Contents

EXECUTIVE SUMMARY .....	4
INTRODUCTION: .....	6
OBJECTIVES .....	9
1. TOP CANADIAN SCAMS .....	10
A. Pretender invoices:.....	10
B. Computer viruses: .....	11
C. Phishing.....	12
D. Advance fee .....	13
2. ROMANCE SCAMS .....	15
A. An introduction:.....	15
B. The anatomy.....	19
C. In numbers .....	21
3. FIGHT AGAINST DOT-CON .....	28
A. Underreporting.....	28
B. Victimization.....	29
C. Victims and society fighting back.....	30
D. Recourses .....	32
4. CANADIAN LAWS AND AGENCIES.....	34
A. An Introduction.....	34
B. Canadian Anti-Fraud Center (CFAC).....	36
C. Financial Transactions and Report Analysis Centre of Canada (FINTRAC).....	37
5. MULTIJURISDICTIONAL CRIMES .....	40
A. MLAT and other requests .....	41
B. INTERPOL and Europol.....	42
C. Council of Europe's Convention on Cybercrime .....	43
6. ROLE OF AN IFA .....	46
A. Compliance monitor for MSP.....	47

B. Disruption program analyst..... 49

C. Online dating fraud detection..... 51

7. FUTURE FRAUD TENDENCIES ..... 52

CONCLUSION..... 54

APPENDIX A - EXAMPLES OF DOT-CON ..... 56

APPENDIX B - COMPANY REACTION..... 60

BIBLIOGRAPHY..... 61

## **EXECUTIVE SUMMARY**

The evolution of the forensic accounting field is inextricably tied to that of frauds and their underlying laws - and with time, these change with the introduction of new technology. The current speed with which technology is being introduced across the world, almost simultaneously, has reduced the physical divide between the scammers and their potential victims via the use of the internet. The constant bombardment of offers of love and prizes have almost made us inure to the fact that this should not be normal.

The availability of this very affordable technology has created a new breed of fraud, that like viruses, have taken the world by unawares and is spreading at an alarming rate. Millions of dollars are lost annually in Canada due to online frauds and on an international level, it translates into billions of dollars in profit to scammers.

This paper will outline a few of the most popular 'dot-con' frauds and how they operate, as well as an in-depth look at the romance scams that have been topping the newswires. The paper will explore the reasons for which the scam has proven to be such a success and the obstacles that victims face due to the transnational nature of the crime.

A brief overview of the Canadian law system and the two main Canadian agencies tasked to fight fraud is introduced. Their interaction with some of the international committees that have been created to tackle this online phenomenon is discussed.

And lastly, a look at the developing roles that the IFA profession could possibly undertake in this new era of the dot-con includes elements of proactiveness that need to be explored.

## INTRODUCTION:

The Merriam Webster defines the "confidence man", or informally the "conman", as "a dishonest person who uses clever means to cheat others out of something of value".<sup>1</sup> While the Oxford Dictionary defines it as: "a man who cheats or tricks someone by means of a confidence trick".<sup>2</sup> It seems ironic that someone that should deprive you of something be associated with the word confidence but that is what needs to be achieved in order for anybody to give up something worthwhile. The word "confidence" qualifies not the perpetrator of the trick but the psychological mental state of the defrauded person - the latter believes the former and agrees to an exchange of something, whether it be a product, service or the promise of love.

With the advent of the computer, smartphones, the internet and the rapid growth of infrastructures to make these technologies available to everyone, a much larger market has opened up to these conmen than in the olden days when a confidence trick would require more time and effort to achieve. Depending on the type of con, the length of time required could take just as long in the present than it did in the past, but the access to the money (which is the usual goal of conmen) is almost instantaneous nowadays and can be done with relative anonymity. There is also the provided luxury of running several cons at the same time at virtual no cost or risk as the current laws have not yet, or do not seem to have caught up with the ever changing technologies. The "term confidence man was probably first coined by the New York press in 1849"<sup>3</sup> but a new term has started to emerge, one that is representative of the technology age: the

---

<sup>1</sup> <http://www.merriam-webster.com/thesaurus/confidence%20man> accessed on June 2, 2015

<sup>2</sup> <http://www.oxforddictionaries.com/definition/english/conman> accessed on June 2, 2015

<sup>3</sup> Halttunen, K. "Confidence Men and Painted Women", p 6 Yale University Press, 1982

"dot-con", or some variation of it, which is different from the dot-com. The excerpt below taken from the Techopedia website provides a good contrast between the two:

**"Definition - What does *Dot-Con* mean?"**

Dot-con is a term for fraud that occurs in an online or digital environment. It can be used for many different kinds of fraud and is a play on "dot-com," a term that is often used to refer to anything related to the Internet.

Journalists and others have used the term dot-con when referring to mass phenomena, such as market trading mishaps, data theft or credit card fraud. The term has also been used to refer to the now infamous tech bubble of the budding 21st century global market. In this instance, dot-con refers to large numbers of investors that lost money in tech-related trading and the sudden re-evaluation of tech companies.

Other references to dot-con may be specific individual instances, in which a consumer, investor or group of people are conned. Some of these are related to the faceless aspect of e-commerce, where scammers can easily bilk customers and set up fraudulent transactions. These types of fraud vary widely, from phishing attempts to the sale of poor quality goods or solicitation of money for goods and services that are never provided."<sup>4</sup>

The term and its definition is still relatively new and has not been added to any dictionary yet but has been used as the title ("Dot.Con") of a recent CBC "DocZone" episode that aired in 2014 and re-aired on June 4, 2015. It is the viewing of the original episode that enlightened me to this

---

<sup>4</sup> Janssen, C.Corey Janssen <http://www.techopedia.com/definition/23397/dot-con> accessed on April 7, 2015

growing category of scams<sup>5</sup> and the large varieties of online scams currently being exploited. I had had prior general knowledge of the different scams outlined in the episode and have even been the recipient of many of the top ten 2013 and 2014 scams, however there existed a vast chasm when it came to numbers - the sheer number of people that have fallen for these scams and the dollar value of the losses that are estimated to have been stolen was almost unfathomable.

---

<sup>5</sup> Defined by the Merriam-Webster as: "a fraudulent or deceptive act or operation" <http://www.merriam-webster.com/dictionary/scam> - accessed on June 3, 2015



## OBJECTIVES

This paper will outline the most popular online scams that have topped Canada's list for 2013 and 2014, with an in-depth look at the #1 scam (dollar wise)<sup>6</sup> that might be slated to remain there for 2015: romance scams.

- The anatomy of the romance scam will be examined through a compare and contrast exercise of testimony from victims - these testimonies will be in summary form and were open-sourced through online chat forums, newspaper articles and the DocZone episode.
- Due to the large impact these scams have had on society, there have been an exponential increase in activities, both private and governmental, in trying to curb the number of victims via education, legal recourses and other methods. An overview of these activities and material will be introduced and the role of an IFA (Investigative Forensic Accountant) in these activities will be examined.

The terms scams and frauds will be used interchangeably, as well as scammers and fraudsters, throughout this paper.

---

<sup>6</sup> As of 2011 - according to the Canadian Anti-Fraud Center (CAFC) "<http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/types/romance-rencontre/index-eng.htm>" - accessed on June 3, 2015

## 1. TOP CANADIAN SCAMS

The Better Business Bureau (BBB) is an organization that operates in North America (Canada and the United States) to ensure fair business practices in order to protect the consumer. It is a different entity from the Competition Bureau, which is a governmental entity that has the role of enforcing fair business practices as well as the protection of the public. Both entities work together in the publishing of an annual list of the top scams that have affected Canadians. The following frauds that ranked within the top ten in 2013<sup>7</sup> and 2014<sup>8</sup> were selected as I was either a first-hand or second-hand recipient of the scam "invitation" in the past few months. I term it an invitation as the scam is presented in the form of a prompt and required participation on my end.

### **A. Pretender invoices:**

There are a few variations to this scam and the more popular ones either require the recipient to make a payment for services/goods that were never rendered or has some type of malware<sup>9</sup> attached to the invoice and gets downloaded into the recipient's computer without their knowledge. The loss that is created from the latter scheme is greater than the payment of a false invoice as sensitive information can be captured and further used by the scammers. The information that is gathered could be as wide-ranging as the simple capture of login usernames and passwords to email accounts, to confidential banking information and social security numbers - which will allow for the illegal transfer of funds and identity theft. This scam is sent in the form of an email with a fake address that has either the vendor name or an authorized

---

<sup>7</sup> <http://www.cbc.ca/news/canada/british-columbia/top-10-scams-of-2013-1.1328875> accessed on May 5, 2015

<sup>8</sup> <http://www.bbb.org/mbc/news-centre/news-releases/2014/02/2014-top-ten-scams/> accessed on May 5, 2015

<sup>9</sup> <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03074.html> accessed on May 5, 2015

superior's name in it, which creates a sense of security in the authenticity of the source. The target of this scam is largely companies as more monies could be obtained and the vast amount of information that is contained on their mainframes is highly valued.

### **B. Computer viruses:**

This type of scam usually comes in the form of a "pop-up" window that will alert you that your anti-virus software has detected a virus while you are visiting a website. These alerts will require you to take immediate action by clicking on a "fix" button and this will allow the scammer access into your computer with or without your knowledge of it. One variation of this scam will require you to provide payment information for the fraudster to "fix" your computer while another will download malware in the form of a Trojan horse virus that will allow the fraudster to access information at a later time. Like the pretender invoice scam, the consequences to the victims are the same.

The reason there are so many victims that fall prey to this particular scam is ironic as it is actually due to the knowledge that there are so many viruses out there and the fear of getting infected. Newer forms of this scam include ransomware which "typically disables a victim's device until a fee is paid to release it."<sup>10</sup>

---

<sup>10</sup> The internet organised crime threat assessment (iOCTA) 2014, page 24  
"<https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta>"

### **C. Phishing**

The most common type of this scam involves an email that appears to come from a financial institution or the tax department requiring them to confirm or validate their information via a provided link - however, they get redirected to a fake website that will capture the relevant information, thus providing the scammer everything they need to access your account or resell that information.<sup>11</sup>

Victims of these scams often react with less caution as there is an instant trust in the source of the email and the fear of an interruption of service that is often time-consuming to rectify. There is also the added sophistication of the scam, where the provided link is a carbon copy of the financial entity's website, lowering even further the victim's guards.

A new variation of this scam that is impacting the youth is called the "insta-scam" - this involves claims of prizes offered by retailers by filling out surveys and inadvertently releasing credit card information<sup>12</sup> or applying for a credit card that will never reach them, which will be used by the scammers.

---

<sup>11</sup> Ibid iOCTA Threat Assessment, page 45

<sup>12</sup> Ibid BBB Top Ten Scams

## **D. Advance fee**

The number of permutations that this scam presents itself is quite large but the underlying principle remains the same: a cycle of payments and disappointments where the ultimate object never gets delivered due to unforeseen circumstances and terminates only when the victim realizes that they've been had or until the fraudster can no longer obtain any further advantage from their victim.

One of the earliest documented form of this scam is called the "Spanish prisoner" and appeared in a New York Times, March 20, 1898 article. The article clearly outlines the way this scam operates - from the receipt of a foreign cry for help, to the reward of money or hand-in-marriage if they help finance the various steps that seem to be plagued by bad luck.

Very little has changed in the *modus operandi* of the advance fee scheme since the 1800's and is now commonly known as the "419-scams", due to the large frequency of perpetrators originating from Nigeria and refers to the country's Criminal Code section on fraud<sup>13</sup>. One of the more popular variant comes in the form of an inheritance scam where the would-be victims will receive emails from "barristers" identifying themselves as representatives of a large estate of which the victim might be the main beneficiary or the beneficiary needs their help to get the inheritance due to governmental red tapes. The reason why so many fraudsters operate out of Nigeria will be addressed in a later section of this paper.

---

<sup>13</sup> <http://www.interpol.int/Crime-areas/Financial-crime/Fraud/419-fraud>

Another trend is in the form of an offer of employment - potential employees are enticed with large salaries with a minimal set-up fee or are paid up-front with a non-sufficient funds (NSF) cheque that is greater than the paycheque amount and are advised to transfer the difference to another account for simplicity purposes.

Examples of these scams can be found in Appendix A - notice the spelling errors and ungrammatical sentences that are commonly found in most correspondence of this type.

## 2. ROMANCE SCAMS

### **A. An introduction:**

This type of scam has been making headlines recently due to the large number of purported victims and the average monetary losses suffered on an international level. According to a report prepared by the International Mass-Marketing Fraud Working Group (IMFWG)<sup>14</sup> in 2010, many victims do not make a report for the money that is lost to local authorities thus the data that has been amassed provides an incomplete picture of what the true number of victims and monies lost are. In a recent interview with a member of the Canadian Anti-Fraud Center (CAFC) team indicated that this statement remains true and estimates that as low as 5% of romance scams get reported. Even with such a low reporting rate, the results in terms of number of victims and amount of reported loss is quite staggering.

A CBC article<sup>15</sup> dated September 2013 reported the following figures that were provided by the CAFC (Stats collected up until Sept. 9, 2013) :

---

<sup>14</sup>" Consists of law enforcement, regulatory, and consumer protection agencies from seven countries, including Australia, Belgium, Canada, the Netherlands, Nigeria, the United Kingdom, and the United States, as well as Europol" - June 2010, A Threat Assessment, "[http://www.fincen.gov/news\\_room/rp/reports/pdf/IMMFTAFinal.pdf](http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf)" - accessed May 5, 2015

<sup>15</sup> <http://www.cbc.ca/news/canada/british-columbia/man-duped-500k-in-online-romance-scam-1.1870043> - accessed on May 5, 2015

	<b>Complaints</b>	<b>Victims</b>	<b>Dollar loss</b>
<b>2013</b>	1,167	744	\$ 9,547,672.73
<b>2012</b>	1,649	1,191	\$16,576,186.74
<b>2011</b>	1,358	935	\$11,771,434.99
<b>2010</b>	914	624	\$ 6,836,801.51
<b>2009</b>	566	375	\$ 3,272,330.06
<b>2008</b>	50	43	\$ 632,731.45

The numbers reflected an alarming trend, whether more victims were reporting their losses or the number of victims have increased from year to year, the public and various agencies have taken notice.

The person in the CBC article was defrauded by someone he met and fell in love with when he signed up with an online dating site - which has been a common story. Initial contact is made on these legitimate businesses but move off to other forms of communications, like email and texting as they know that communications within the dating website may be monitored. In this case, the victim was being lured by two conmen working together and thru the help of a private investigator, one may have been brought to justice but the recovery of the money is not something the victim believes will ever happen.

The anonymity that these online websites provide works very well for fraudsters who try to draw in as many victims as possible. The set-up of multiple fake profiles, with different pictures to attract all types have provided the fraudster with tools in their arsenal that were not possible in the past. Not all contacts on the dating sites lead to romances, some lead to friendships and from these friendships, fraudster may be able to glean additional information that they then use to



create a "perfect mate" that will lull the victim even further into the trap, all without having an accomplice - the fraudster will play the role of the friend and lover simultaneously as everything is done over the internet.

Another romance scam that has been gaining a lot of momentum have been termed "army/military scams" as they usually involve the setting up of profiles using US soldier pictures and claim that they are fighting wars overseas and require the help of their new found love to get their release papers and set up new business opportunities. One such victim believed that she had become engaged to a soldier that she met through a dating website. Small gifts had been exchanged and a fake diamond ring was used in the proposal. However, her story does not end with only the lost of money - she was allowed the opportunity to meet her lover online in the form of a taunt: "a 22 year old Nigerian kid".<sup>16</sup> The taunts then escalated to blackmail as intimate pictures were shared, the blackmailing would include the request to lure other potential victims, and although she has not participated, her pictures are being used as bait.

Another victim mentioned in the same article met her scammer through "Skype" after she had been sent several requests to chat - she wasn't looking for love or friendship but fell for the perfect man and went as far as travelling to another country to remit money to a third person so as to bypass any traces of a money-trail. What isn't highlighted in the article is that there is a chance that these women could be arrested for crimes they didn't even know they had committed: money laundering being a very real possibility.

---

<sup>16</sup> Power, J., "Love me don't: the West African online scam using US soldiers", December 6,2014  
"http://www.smh.com.au/good-weekend/love-me-dont-the-west-african-online-scam-using-us-soldiers-20141204-11szid.html" - accessed May 14, 2015

Finally there are romance scams that could lead up to a business relationship - as was the case of the victim in the Dot-Con program. She had met her business partner on a dating website and the perfect mate presented himself as a knowledgeable mortgage broker and hired her to create a website for his business. She fell into his schemes when he had asked to advance money on a purchase for which the mortgage will not be cleared in time - the only difference between her story and those before is that she had met her fraudster in person.

In the last story, the scammer is a wanted person that had previously been charged for fraud in Canada but remains at large, living off of women's generosity and his ability to charm them into believing that he is a successful man and a trusting person.<sup>17</sup> Although, he doesn't fall within the growing trend of online scammers operating in foreign countries, the genesis of the scams were the online dating websites, only his stories took on more traditional undertones.

The phenomena of using another person's pictures to create a fake online identity is so rampant that a new term has been coined for these people - "catfish". The term entered the urban dictionary in 2010 after a documentary film, after the same name, was released by the victim that was duped into having a relationship with someone that turned out to be someone else. The relationship was initiated and bloomed online via "Facebook", where the catfish created several fake profiles to interact with the main character. The reason the other profiles were created was to reinforce that the catfish really did exist and acts as confirmation that their backstories are true or verifiable.

---

<sup>17</sup>Quinn, J., "Online dating relationship ends badly, \$1.3M later" The Star, November 30, 2013  
"[http://www.thestar.com/news/world/2014/02/06/the\\_cost\\_of\\_love\\_alleged\\_fraudster\\_leaves\\_broken\\_hearts\\_empty\\_bank\\_accounts.html](http://www.thestar.com/news/world/2014/02/06/the_cost_of_love_alleged_fraudster_leaves_broken_hearts_empty_bank_accounts.html)" - accessed May 15, 2015

This type of social engineering, referred to as "the act of manipulating people into performing actions or divulging confidential information"<sup>18</sup> is not limited to romance scams, but is a key characteristic of all dot-cons. Information has always been valuable and their ability to extract and use that information in the digital age has grown exponentially.

## **B. The anatomy**

A psychology study by University Professor Whitty outlines that a romance scam is actual two scams that are operating simultaneously: there is an element of identity fraud and then there is the mass marketing fraud<sup>19</sup>.

Being a catfish would fall under the identity theft element but what is mass marketing fraud (MMF)? The Competition Bureau defines it as knowingly making materially false or misleading representations using mass communication media (the telephone, mail, and the Internet)<sup>20</sup> to defraud the public. For the victims of romance scams, the love that is promised never gets delivered - making this an advance fee scam and a MMF. As a matter of fact, all of the dot-cons that were discussed so far fall under the general term of MMF and is being monitored by government bodies across the world.

---

<sup>18</sup>Europol, Threat Assessment (Abridged)- Internet facilitated organized crime (iOCTA) July 2011, page 7

<sup>19</sup> Whitty, M "The Psychology of the Online Dating Romance Scam" - April 2012

<sup>20</sup> <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/02775.html> - accessed May 15, 2015

The Whitty paper also outlines the risk of the same victims falling prey to a secondary scam, in which collaborators would present themselves as investigators<sup>21</sup> able to recover the loss monies or bring the fraudster to justice, which would then lead to more heartache and monetary losses.

The losses that arise from romance scams are so large because the victims are often emotionally invested in the relationships, even when they were not looking for one, and are victims due to some vulnerability at the time of the encounter, not because they were gullible or uneducated. The scammers work on finding out those vulnerabilities and exploit them.

---

<sup>21</sup> Ibid Whitty (2012), pages 6-7

## **C. In numbers**

The Canadian Anti-Fraud Center (CAFC) is a governmental agency, set up in 1993, to help amass information on various frauds that fall within the Canadian border and help investigative bodies by providing them with data and analyses.<sup>22</sup> They keep track of activities that victimize Canadians as well as those who perpetrate the acts within Canada.

The following figures were amassed by the CAFC and show the continued growing trend of romance scams<sup>23</sup> and their target age group in Canada:

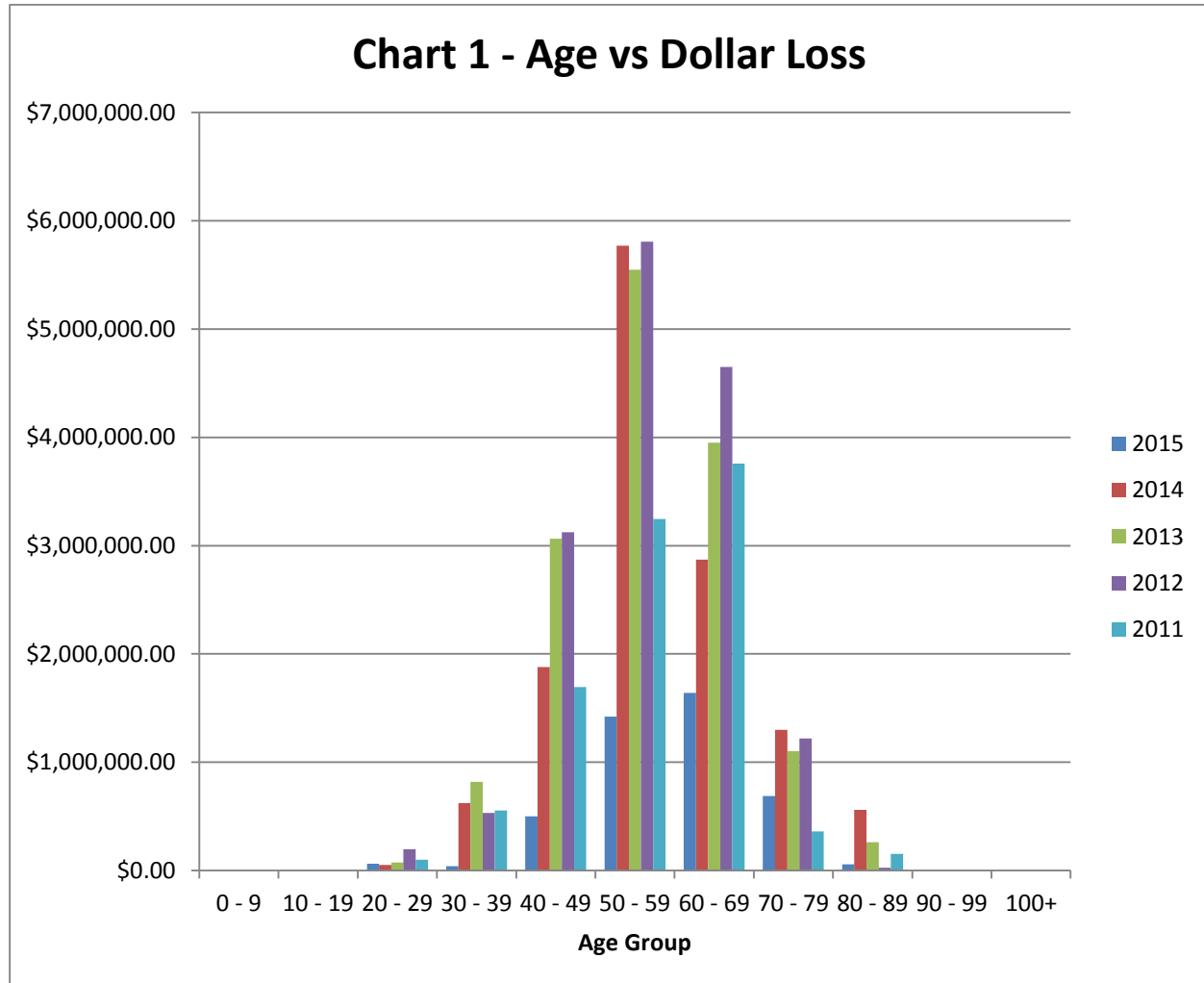
### **1. A comparative look at the reported monetary loss between 2015 (April) and 2011**

<b>Age Range</b>	<b>2015</b>	<b>2014</b>	<b>2013</b>	<b>2012</b>	<b>2011</b>
0 - 9	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
10 - 19	\$0.00	\$1,350.00	\$0.00	\$0.00	\$0.00
20 - 29	\$62,286.86	\$50,318.62	\$74,997.71	\$196,762.38	\$100,517.23
30 - 39	\$39,799.00	\$621,521.25	\$817,468.23	\$530,910.85	\$554,820.88
40 - 49	\$500,388.27	\$1,878,524.15	\$3,064,047.85	\$3,123,386.14	\$1,693,841.58
50 - 59	\$1,420,226.75	\$5,769,226.45	\$5,547,298.27	\$5,807,311.53	\$3,245,589.35
60 - 69	\$1,640,058.72	\$2,871,612.77	\$3,950,608.99	\$4,650,382.51	\$3,758,226.98
70 - 79	\$689,315.50	\$1,297,854.70	\$1,102,098.88	\$1,218,754.54	\$360,862.22
80 - 89	\$57,391.30	\$560,961.12	\$261,289.98	\$25,160.35	\$153,133.00
90 - 99	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
100+	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>Total</b>	<b>\$4,409,466.40</b>	<b>\$13,051,369.06</b>	<b>\$14,817,809.91</b>	<b>\$15,552,668.30</b>	<b>\$9,866,991.24</b>

Represented in a graph format:

<sup>22</sup>"<http://www.antifraudcentre-centreantifraude.ca/english/stopit-faq/html>" - accessed April 7, 2015

<sup>23</sup> Due to online scams



What is apparent from the graph above is that the victims that have lost the most money are those that are close to the age of retirement(50-59) or have already retired (60-69) and have been drawing on their life savings and taking on new debt in form of mortgages, borrowing from friends and family and cashing in their retirement savings in order to keep their newfound love happy. This creates societal strains as victims usually suffer the immediate backlash for not being able to pay back the sums that are borrowed from friends and family and could face foreclosure when the mortgage payments can longer be sustained.

For the last 3 years (not including 2015) more than \$10 million have been lost - loosely extrapolated, if these figures represent only 5% of the total losses, then on a yearly average, over \$200 million might have been lost to romance scams alone. This may seem like a preposterous figure but a recent report by an Australian government agency indicates that as much as \$25 million were reported to be lost annually due to online romance scams alone,<sup>24</sup> therefore an estimated actual loss of \$200 million may not be so farfetched after all.

The reason the losses are so great in the population that is greater than 50 years old is due to a multitude of factors. Many are actively looking for love when they sign up to these dating services after being widowed or divorced and believe that it will be easier than trying to strike up a conversation with a stranger in a bar setting. They may not be hopeful that something could happen but there is no risk to try right? The known *modus operandi* of these scammers is to bombard potential victims with affection so that they feel a connection, and the contact is constant so that the affection can build - this is how all romance scams occur but in the online world, a whole team of scammers work together and the victim is usually conversing with more than one person who plays the role of the love interest for several months. The "business of romance" is so lucrative that many law enforcement agencies believe that they are dealing with an organized crime unit<sup>25</sup>. The script that these fraudsters use are all variations of one another but essentially boils down to an advance fee fraud where a little more is asked each time and the threat of losing a lover keeps the victim from breaking off these 'relationships' and remaining compliant.

---

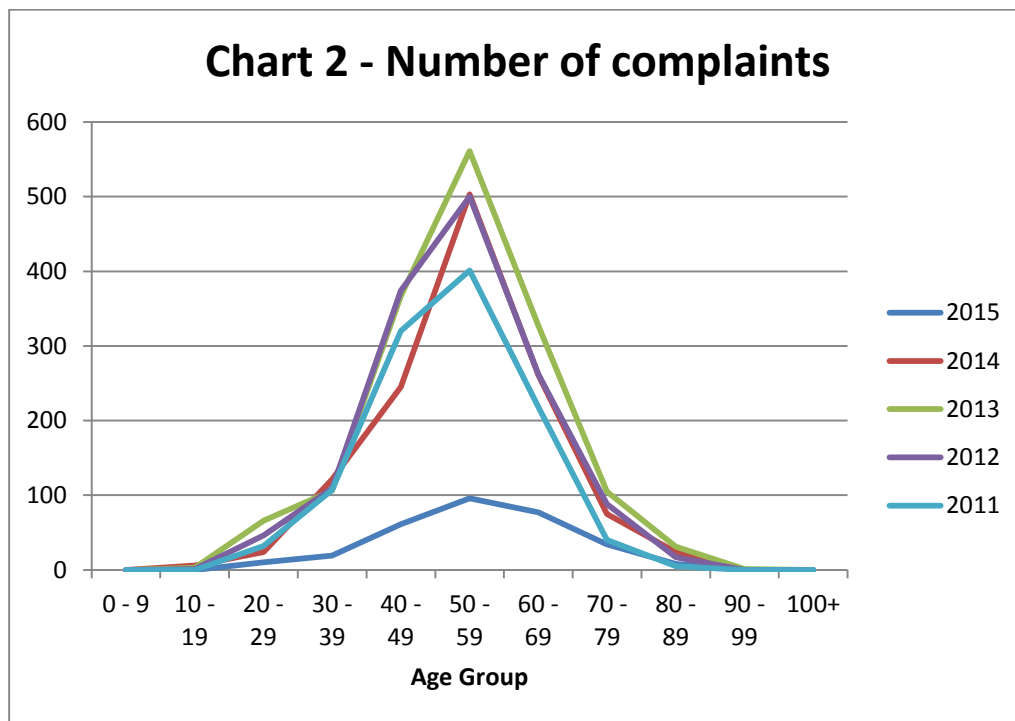
<sup>24</sup> "<http://www.criminallaw.com.au/blog/criminal/general/online-love-predators-raking-in-millions/35323>" - accessed June 4, 2015

<sup>25</sup> Ibid Quinn, J (2013)

**2. A comparative look at the number of complaints between 2015 (April) and 2011**

Age Range	2015	2014	2013	2012	2011
0 - 9	0	0	0	0	0
10 - 19	0	6	3	1	0
20 - 29	10	24	66	46	32
30 - 39	19	121	106	109	107
40 - 49	61	245	367	374	320
50 - 59	96	503	561	500	401
60 - 69	77	261	327	262	218
70 - 79	34	75	105	88	40
80 - 89	8	24	31	17	5

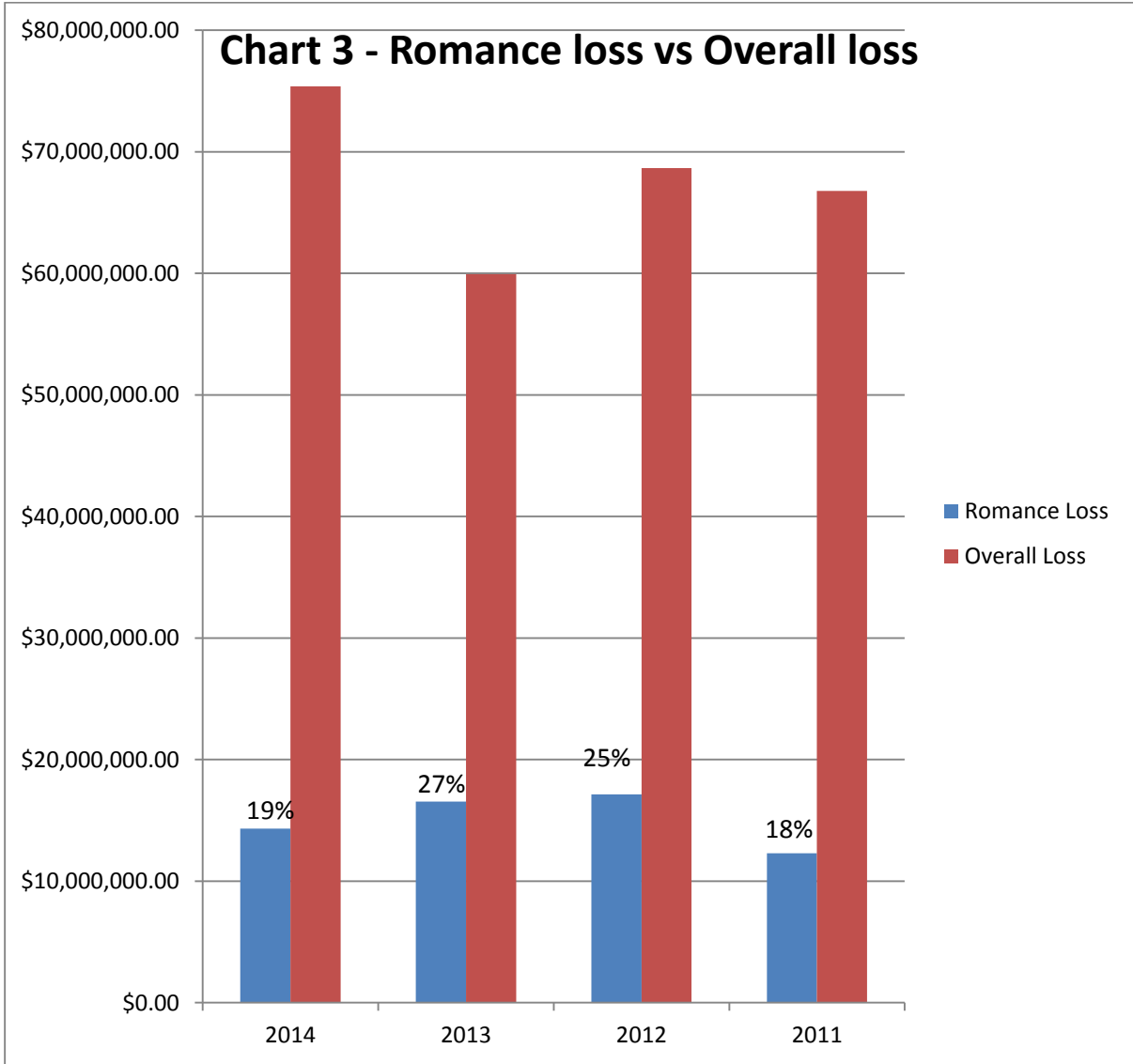
Represented as a graph:



The trend that Chart 2 shows is congruent to Chart 1, with respect to the impact per age group - which is to be expected. However, what can be gleaned at a first glance is that the number of complaints seem to have staggered since 2013, although the aggregate monetary loss is greater in 2014 for that same age group, which means on average, more money was lost per individual.



**3. A comparative look at monetary loss from online romance scams as a percentage of overall scam loss between 2014 and 2011**



	Romance loss	Overall Loss	% of Overall
2014	\$14,315,644.38	\$75,386,952.83	19.0%
2013	\$16,538,697.54	\$59,930,887.77	27.6%
2012	\$17,132,898.85	\$68,646,695.07	25.0%
2011	\$12,290,790.49	\$66,769,038.24	18.4%

The data for Chart 3 for the overall losses that were compiled reflect the reported losses for individuals to all MMF-type scams by the CAFC. The graph depicts that about a quarter of the funds that are lost are a result of romance scams. Although this picture is by no means complete it is representative of the growing impact romance scams have had on Canadians.

Internationally, figures that are being reported mirror the growing trend that is illustrated in the data gathered.

- In the United States, the reported losses from romance scams have grown at exponential rates, with the latest estimate by the FBI of some \$84 million in the last six months of 2014<sup>26</sup>. While the Internet Crime Complaint Center (IC3) released that over \$56 million was reported to be defrauded from its citizen in 2012 by romance scams<sup>27</sup>, representing

<sup>26</sup>Shadel, D. and Dudley, D., "Are you real? - Inside an Online Dating Scam" AARP Magazine, June/July 2015  
["http://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html"](http://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html) - accessed June 13, 2015

<sup>27</sup> Johnson, M. A., NBC News "Older women most likely to click with online romance scam artists" May 14, 2013  
["http://usnews.nbcnews.com/\\_news/2013/05/14/18255848-older-women-most-likely-to-click-with-online-romance-scam-artists?lite"](http://usnews.nbcnews.com/_news/2013/05/14/18255848-older-women-most-likely-to-click-with-online-romance-scam-artists?lite) - accessed May 15, 2015

10% of all internet scam losses, which was a small increase over the \$50.4 million that was reported in 2011<sup>28</sup>.

- In the United Kingdom, actual recorded instances of romance scam for 2014 were 2,503 but the National Crime Agency estimate that there could be as many as 200,000 victims with a collective loss of £100 million annually.<sup>29</sup>
- In Australia, the 2013 losses of \$25 million due to romance scams made up about 30% of its reported \$89 million losses from online scams, despite representing only 3% of the reported scams to the Australia Competition and Consumer Commission (ACCC).<sup>30</sup>

---

<sup>28</sup> Hicken, Melanie, "I was a victim of an online dating scam" February 20, 2013, CNN Money <http://money.cnn.com/2013/02/20/pf/online-dating-scam/> - accessed May 24, 2015

<sup>29</sup> National Crime Agency (2014), "<http://www.nationalcrimeagency.gov.uk/news/news-listings/478-romance-fraud-mastermind-jailed-in-ghana>" - accessed June 4, 2015

<sup>30</sup> Simpson, Campbell "Scammers took \$89 Million from Australians in 2013" June 16, 2014 <http://www.gizmodo.com.au/2014/06/scammers-took-89-million-from-australians-in-2013/> - accessed June 4, 2015

### 3. FIGHT AGAINST DOT-CON

Public awareness has been steadily increasing with the weekly headlines and in depth documentaries and the incessant barrage of spam emails but then why are there still incidences of underreporting? What are the stigmas that are attached to the victims and what are their recourses?

#### **A. Underreporting**

Victims are often in an even more vulnerable state after they find out they have been taken in and may fear either that 1) no one would believe them, or even if they did, 2) that there is nothing that can be done as the money was surrendered willingly - as was the case of a woman who tried to report the incidence to her local police.<sup>31</sup> If the people who are supposed to reinforce the law don't know or understand it, then how can the public recognize it to report it effectively?

Criminal investigations are usually undertaken at the discretion of the prosecutors and whether they believe that they can recover loss funds or try the criminals to keep them from harming the public. In online scam situations, where the perpetrators are not even in the country and very little may be recovered, there will not be a large motivation for them to even look at a case where the individual's loss is less than \$20,000<sup>32</sup> as the associated court fees would be greater.

Therefore why would the average person make a complaint if it will not lead to any justice?

---

<sup>31</sup> Stevens, C., "Online romance scams bilk Canadians out of nearly \$14M in 2014", Global News, March 9, 2015 "<http://globalnews.ca/news/1873036/online-romance-scams-bilk-canadians-out-of-nearly-14m-in-2014/>" - accessed May 31, 2015

<sup>32</sup> Per CAFC 2014 stats: loss per person in overall MMF funds in Canada is \$3,406 on average and for romance scams \$15,935 on average

Under common law, the victims will have to take private measures to court and try to recover the monies that are lost, which would also be seen as a loss of time and effort as well as money as the probability of ever recovering the awards from a foreign, unknown, person is next to nil.

However, there are other statutes under which the fraudster can be persecuted - such as the Competitions Act if they are running a business, or a legislative body if they claim to be a professional that belongs to an Order or Association as they all have defined standards and penalties for fraudulent acts. The public may not be aware of these other recourses but by filing a police report will increase the chances of some other agencies taking cognizance of it and taking the required steps to start an investigation or drawing a link between crimes happening in different jurisdictions.

## **B. Victimization**

Under both the Canadian common law and criminal code, fraud is an offence that is punishable by fines and sentencing but the disparity between the punishment and the victim's losses may be enough to discourage even the staunchest victims. To illustrate this point, there is a recent case<sup>33</sup> of a Vancouver romance scam artist, who is a repeat offender, that had received multiple jail sentences in the last 10 years spanning several months to a maximum of 5 years. Jail time has not deterred him nor changed his attitude but the impact to his victims will probably last longer than his sentences put-together.

---

<sup>33</sup> Fumano, D., "Con man 'could talk fleas off a dog' but he's messed with the wrong girl", July 5, 2013, The Province, "[http://www.theprovince.com/story\\_print.html?id=8612967&sponsor=escapes.ca](http://www.theprovince.com/story_print.html?id=8612967&sponsor=escapes.ca)" - accessed May2, 2015

Criminal cases are public domains and although the names of the victims may be subject to publication bans, they know who they are and when their cases are reported on news websites, there will always be commentators that will call them "stupid, gullible, greedy" and more often than not, those same sentiments are projected by the police officer that is taking down their reports. As commented by a CAFC member, a "buyer beware" mentality can be adopted by law enforcement and very little empathy is given to the victims. With these types of stigma dogging the victims, very few will acknowledge the fact that they had fallen prey to these type of scams, which is another factor for underreported cases.

The Whitty study indicates that the victims experience psychological impacts that are similar to Kubler-Ross's (1969) stages of grieving which make them prone to being re-victimized or depressed to the point of having suicidal thoughts<sup>34</sup>. This is another side effect of these scams and the authorities that deal with the victims may not understand that health professionals should be recommended.<sup>35</sup>

### **C. Victims and society fighting back**

The common undertone that is being brought to light in all of these recent articles is the hope that their stories would help others come forward to report their victimization, to enlighten them to the fact that they are not alone and should not feel ashamed and help educate the general public as to the real consequences of these scams. Furthermore, there is also the fact that their fights are

---

<sup>34</sup> Ibid Whitty, page 15

<sup>35</sup> Ibid Whitty, page 20

being noticed by the proper authorities and forces them to acknowledge that there is a problem that needs to be addressed.

Several of the women who have been victimized by romance scams have taken action through online medias to alert others as to the dangers of online dating, as well as personally taking charge of contacting other potential victims that might have fallen for the same scammers and are either not aware that they are dealing/dealt with a fraudster or reticent in coming forward. Being contacted by someone who has lived the same story might entice the other victims to be more open to discussing and sharing details than to a police officer who "would not understand".

There exist several online groups whose mission is to educate the public of ongoing romance scams. These websites are essentially for informational purposes but also provide a support system for victims and links to the proper authorities to contact to report the losses if they had not done so already. An online community is thus created and information that might not have been easily accessible suddenly become available to everyone. The information can be in the form of fake identities, including name and back stories of the fraudster to the pictures that are the most popular for catfishes to use and can even go as far as other victims describing how they were duped and the actual correspondence that was sent by the fraudster as they have a tendency to recycle the same material.

Other websites offer their members the possibility of "scamming the scammers" by posing as bait so as to tie up their efforts and dwindle the actual number of real victims. These websites do not investigate scammers, nor do they defraud the scammers. Their sole purpose is distract real

fraudsters by keeping them interested with ploys and promises of monies that do not get delivered. When they think that they have potential information that could be relevant to a law enforcement agency, then that information is passed along, so that proper action can be taken. These websites also provide information on the types of scams that are ongoing so that every potential permutation is exposed.

#### **D. Recourses**

There is a general acknowledgement throughout the international law enforcement community that there is not enough in place right now to effectively combat these online scams as there are not enough resources. Due to the inherent underreporting of the victims of scams, or the potential of being victimized, the true potential threat is lost on those who allocate the resources.

We live in a society that is resource limited, and instinctively do a cost-benefit analysis to determine how best to use that resource. If the statistics indicate that money and manpower is best served (when considering number of victims, dollar value and societal impact) in cracking down on drug crimes than on online scams, then educating the front-line police officers on the type of drugs and how to profile the distributors will take precedence.

More often than not, the knowledge that is required to track down and analyze the information that is generated by these online scams are so specialized (ie: computer forensic experts) that the common police officer is not equipped with even the basic knowledge to handle that evidence<sup>36</sup>. Furthermore, police officers are not the only ones that are the first point of contact for victims -

---

<sup>36</sup> Ibid iOCTA, Threat Assessment 2014, page 69



the customer service department of service providers also receive complaints but whether and how many recognize that a scam has just occurred and whether that information gets passed on to the proper authorities remain unclear. If there are no policies in place that make it mandatory for these complaints to be reported to the proper authorities, then that information gets lost<sup>37</sup> in the shuffle and the victims may be left to believe that action has been undertaken.

After making an initial report then the proper authorities will hopefully be notified and a course of action to ensure that justice in the form of restitution and punishment of the perpetrators will occur. However, who are the proper authorities and what is the course of action they will undertake?

Furthermore, there are other factors that are just as, if not more important that need to be considered:

- multi-jurisdictional of the transnational nature of the crimes
- the laws in the country where the fraudsters reside and the ability of extradition

The next sections will discuss the obstacles that the legal enforcement agencies and authorities face when fighting online fraud.

---

<sup>37</sup> Ibid, iOCTA (Abridged), page 8

## 4. CANADIAN LAWS AND AGENCIES

### A. An Introduction

Has a crime occurred? What laws were broken and how do you go about reporting it? In Canada, there are several legislative bodies that can bring action against an individual that has broken a law, a code of ethic or regulations. And fraud is one of those instances that seems to be covered by multiple legislative bodies as it violates, in essence, everything.

The Canadian court system is a vestige of both its colonial ancestors in that they have both a common law system (England) and a civil law system (French) operating within its borders. To be able to properly describe the various forms the laws come into being would take several textbook chapters and fall outside the purview of this paper, however it can be summarily said that it is by no means static but any changes to existing laws or the enactment of new laws is a lengthy process. Laws are created or amended to take into account new situations and technologies so as to keep society safe and ensure that all citizens are treated fairly.

However it has oft been criticized that lawmakers have not been able to keep up with the speed at which technologies have developed, sometimes because of conflicts with existing Canadian Charter Rights (Charter). For example, the Charter guarantees a person their right to face their accuser, so if as a Canadian citizen you fall into a romance scam where the scammer is in Nigeria, the Courts request that the scammer be present in court (in Canada) before the trial can proceed further. This could mean that the victim will have to fly the scammer into Canada on

their own dime, maybe even several times, for a long court process. Some other countries have similar laws and before they are willing to consider extraditing one of their citizens to Canada to face charges, they require the victims to fly into their jurisdiction to make an official complaint. Both of these obstacles are very real in terms of the further cost it imposes on the victims and the added risks of having to travel to dangerous places. However, such is the nature of transnational crimes - the need to comply and be aware of the laws in several countries.

Another facet of the legal framework are the agencies that are set in place to enforce the laws. Whether laws need to be amended, changed or added are oftentimes a consequence of the public's demand for them or a need that has been identified by the members of the agencies, as a result of extensive dealings with the public and seeing the shortcomings of certain laws or lack of any. One such category of laws that came into effect in 2015 is the new cyberbullying legislation<sup>38</sup> - Bill C-13, as a result of recent outcries by parents across Canada after the death of several teenagers and the need for the police officers to gain a different type of access to investigate suspects without violating the privacy laws that are in place<sup>39</sup>.

---

<sup>38</sup> <http://www.getcybersafe.gc.ca/cnt/cbrblng/prnts/lgl-cnsqncs-en.aspx#a02> - accessed June 13, 2015

<sup>39</sup> Government of Canada - Fact sheet: Privacy Protection and the Protecting Canadians from Online Crime Act <http://news.gc.ca/web/article-en.do?ctr.sj1D=&ctr.mnthndVI=11&mthd=advSrch&ctr.dpt1D=6681&nid=832379&ctr.lc1D=&ctr.tp1D=&ctr.yrStrtVI=2013&ctr.kw=&ctr.dyStrtVI=3&ctr.aud1D=&ctr.mnthStrtVI=11&ctr.page=1&ctr.yrndVI=2013&ctr.dyndVI=29> - accessed June 13, 2015

## **B. Canadian Anti-Fraud Center (CAFC)**

Taskforces are used within the business world when there is a need to create an informal body to study an issue that may arise and resources are pooled from various departments. This technique has also been used by the law enforcement community on a national and international scale. One consequence of such a taskforce is the creation of formal bodies when the situation warrants it.

The CAFC, previously known as "Project PhoneBusters", is the end result of a two member taskforce that started out with one Ontario Provincial Police (OPP) officer and an RCMP officer who in 1993 wanted to start keeping track of telemarketing fraud occurring in the North Bay area. But as the project progressed, they realized that the problem was much more widespread and other factions were added to the data gathering task throughout the years - from victim assistance to analytics to disruption initiatives. The Competition Bureau formalized its participation<sup>40</sup> with the Project in 2006 and added mass marketing fraud to their mandate. The disruption initiatives are projects that the CAFC and industry partners develop to make it harder for fraudsters to operate.

The CAFC is Canada's central fraud repository, and it is because it has been tasked to gather all instances of fraud that occurs within our borders that makes it a central figure in the fight against fraud. Other countries work closely with the CAFC to develop agencies of their own in their fight against fraud within their jurisdictions. There are also taskforces that have been created on an international level to combat online fraud due to its transnational nature. These entities enable

---

<sup>40</sup> <http://www.antifraudcentre-centreantifraude.ca/about-ausujet/index-eng.htm> - accessed June 13, 2015

the sharing and information gathered by its members in a way that traditional protocols could not. These transnational entities are forever evolving as it mimics the criminals they are trying to catch.

### **C. Financial Transactions and Report Analysis Centre of Canada (FINTRAC)**

Created in 2000, FINTRAC is a financial intelligence unit that analyzes movement of monies coming in and out of Canada. This type of tracking and analysis is important in order to fight money laundering and terrorist financing on an international level and is relevant to fighting fraud where millions of dollars cross national borders. Some enforcement agencies believe that the heads of the organized crime entities behind the online scams are also terrorists, for example Nigeria's Boko Haram group<sup>41</sup>.

Money laundering is the act of introducing ill-gotten gains into the economic system by masking its origins. In the case of romance online fraud, scammers often require their victims to aid them in their quest to meet face-to-face by sending money to various "associates." In the past, money was sent by cheque or actual cash would be hand-delivered to a third person, nowadays, the method of choice is to wire the money through money service providers (MSP) such as Western Union and Money Gram, as well as through official banking channels.

---

<sup>41</sup> Ibid Shadel, D - June 2015

The government of Canada requires all financial institutions to declare any movement of monies that are greater than \$10,000 to be declared to FINTRAC in their mandate to fight against money laundering. The scammers are well aware of this requirement, as it is one that is adopted by the United States as well and has been effect since 2000, therefore they ensure the amount that is asked fall below this threshold so as to not arouse any suspicion but the use of banking institutions is not their preferred choice as it leaves a paper trail. Banks are further required to keep track of their clients habits and notice suspicious activities that might be a result of money laundering or if they might have fallen prey to scammers overseas. Suspicious activities might include the number of large transactions within a short period of time, or the location to which the money is being wired to if those have been flagged as high risk countries, such as Nigeria, Jamaica or Malaysia<sup>42</sup>.

MSPs are the institutions of choice as they are present all around the world and their compliance with regulations can be shoddy even within controlled environments, like the United States and Canada, therefore one can only imagine their record keeping in more corrupt states. Once the money is sent, there is virtually no paper trail as to who picks it up and whether it was further wired to another location; the only thing that law enforcement knows for certain is the location of where the money was originally wired to. This provides anonymity and insulating scammers and the organization they may be working for.

---

<sup>42</sup> As per interview with CAFC member

FINTRAC is a member of Egmont Group, which is an international cooperative network of financial intelligence units (FIU) and through its membership can trace suspected proceeds of crime across multiple jurisdiction<sup>43</sup>. The collaborative efforts of this group to fight against money laundering by the exchange of timely information is more expedient than formal mutual legal assistance mechanisms in place between the same countries.<sup>44</sup>

---

<sup>43</sup> Egmont Group of Financial Intelligence Units, Annual Report 2012-2013, page 6

<sup>44</sup> An Egmont Group White Paper - "The Role of Financial Intelligence Units in Fighting Corruption and Recovering Stolen Assets", September 2012, page 10

## 5. MULTIJURISDICTIONAL CRIMES

An older story of a German woman who became a victim of a 419-inheritance scam sheds light on how difficult it is to bring someone to justice even if you were able to confront them face-to-face. The story was covered in a 2005 article printed by a Dutch newspaper ("Spiegel International") about the victim's ongoing 13 year battle with the Nigerian courts and fraudster and how she is now advising other German victims on their battles in Lagos, Nigeria. She works as a contractor with the Nigerian anti-corruption agency the Economic and Financial Crimes Commission (EFCC) that was established in 2004. Her story does not start with an online scam as that kind of technology would have been too costly for scammers to use but in 2005, it was perceived that Lagos was the world's leader in internet fraud and the reason is that there is no shortage of individuals willing to make a career out of being a "419-scammer"<sup>45</sup>.

The article outlines a whole infrastructure where scam templates are available for sale and actual office space is rented for the scammers, the "employees" work in shifts to ensure there will always be someone working the different time zones and livings are made by those who have no other opportunities.

The added benefit that they live in a country that is corrupt and that is physically far reaching from the hands of the law of their victim's countries make the "career" even more appealing. The scammer that was interviewed in this article sees his next career move as a script writer, which would be less stressful than trying to run several cons at the same time.

---

<sup>45</sup> Buse, U., "Spam Scams: Africa's city of cyber gangsters" Spiegel International, November 7, 2005  
"http://www.spiegel.de/international/spiegel/spam-scams-africa-s-city-of-cyber-gangsters-a-384317.html" - accessed May 2, 2015



The following sections will examine the measures that are currently in place and available for Canadian law enforcement agencies in their pursuit of transnational crimes. The United States have several agencies in place that deal with online fraud crimes who work in close proximity with their Canadian counterparts - these agencies will not be discussed as the fraudsters usually do not reside in the United States and the obstacles that are encountered with other nations are not the same.

### **A. MLAT and other requests**

Mutual Legal Assistance Treaties exist between countries to help resolve criminal matters that span multiple jurisdictions. The assistance is in the form of evidence gathering, carrying out orders or warrants, transferring of prisoners to help testify or assist and search and seizures<sup>46</sup>. The request for foreign assistance must come from Canada's Attorney General office, which is then communicated to the other country's counterpart body, and is then sent to the agency that holds the required information. These procedures are time consuming and expensive due to the different levels of clearance required and there are no guarantees that the required information can be delivered in a timely fashion as time limitations can only be requested and not demanded. Due to the fast-paced world of online scams if action needs to be taken on a single individual, the information may become irrelevant by the time it does get received.

Less official cooperation can be requested between different nation's police forces if there is no MLAT between the countries, or even if there is one as it will probably be less costly and obtained in a more timely manner. However, the information that is received must meet the

---

<sup>46</sup> <http://www.ppsc-sppc.gc.ca/eng/pub/fpsd-sfpg/fps-sfp/fpd/ch43.html#section43> - accessed May 19, 2015

original country's evidence standards to ensure it is admissible in their courts. In countries, such as Nigeria, where corruption is rampant there is an extra need to corroborate the information by independent means. The RCMP has three liaison officer programs in Africa that could help with the verification and gathering of non-sensitive information but they do not have the power to carry out full investigations as those powers remain with the law enforcement agents of the country.

## **B. INTERPOL and Europol**

INTERPOL is an international police organization with over 190 member countries whose goal is to facilitate police work globally. In addition to being a repository of information that is able to provide training and analyses on growing trends on a timely basis, it also has investigative powers within its member states - while operating within the confines of existing domestic laws. Their mandates are responsive to their member's needs and perceived threats and funding for their activities come in the form of membership dues and donations from both public and private sectors.<sup>47</sup>

INTERPOL divides cybercrime into three broad categories, one of which is financial crimes and corruption - including online fraud. The speed at which the organized criminals are amassing fortunes through the internet has been recognized as being unprecedented.

INTERPOL's initiative to combating cybercrime has led to the creation of the INTERPOL Digital Crime Centre which provides "proactive research into new areas, latest training

---

<sup>47</sup> <http://www.interpol.int/About-INTERPOL/Funding> - accessed June 5, 2015

techniques and coordinates operations in the field."<sup>48</sup> A result of the coordinated operations is the dismantling of criminal networks and arrests of fraudsters for crimes with victims all over the world<sup>49</sup>.

Europol is the European Union law enforcement agency that handles criminal intelligence<sup>50</sup> which has no executive powers but lends support to the EU member's law enforcement agencies with timely information and analyses. Europol's European Cybercrime Centre (EC3) was created in 2013 as a response to the growing trend of cybercrime. An example of the increased importance of transnational cooperation is the recent collaboration between INTERPOL and Europol has brought about the downfall of 118 online fraudsters in the airline sector.<sup>51</sup> The operation traced the purchasing of airline tickets with stolen credit card information and involved more than 60 airlines. This collaborative effort involved representatives from major credit card companies as well as the International Air Transport Association (IATA), which highlights the need for the private sector to aid law enforcement agencies in their aspiration to make "cyberspace as crime free as possible for global citizens."<sup>52</sup>

### **C. Council of Europe's Convention on Cybercrime**

Other international conventions have cropped up over the years to combat cybercrime - which is defined as anything relating to criminal activity which uses computers and online scam activities definitely falls under this grouping. Canada is a signatory of the Council of Europe's Convention

---

<sup>48</sup> <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> - accessed June 5, 2015

<sup>49</sup> <http://www.interpol.int/Crime-areas/Cybercrime/Operations> - accessed June 5, 2015

<sup>50</sup> <https://www.europol.europa.eu/faq#n77> - accessed June 5, 2015

<sup>51</sup> <http://www.interpol.int/News-and-media/News/2014/N2014-228> - accessed June 5, 2015

<sup>52</sup> Ibid, INTERPOL.

on Cybercrime, which has the mandate to "pursue a common policy aimed at the protection of society [...] by adopting appropriate legislation and fostering international cooperation"<sup>53</sup> By promoting common policy amongst members, it will allow for an easier sharing of information and prosecution of criminals.

The articles set out in the convention, known as the Budapest convention, address legal elements that have to be either created or adapted into the signatories domestic laws (Chapter II), as well as principles relating to international cooperation (Chapter III) , a few of which we will further explore:

- Article 24 - Extradition, paragraph 1a) "[...] criminal offences established in accordance [...], provided they are punishable under the laws of both Parties"<sup>54</sup> is called into attention as a country whose laws have not been modernized to include offences covered by the cybercrime convention, then there could not be extradition requests even if the scammer has been identified and within the grasps of multiple law enforcement agencies.
- Article 25 - General principles relating to mutual assistance, paragraph 5) [...] the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence [...] if the conduct underlying the offence for which assistance is sought is a criminal offence within its laws."<sup>55</sup> This outlines the difficulties that the users of mutual legal assistance have had in the past in their dealings with countries that require dual criminality - a memorandum prepared by

---

<sup>53</sup> Council of Europe (2015), "<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>" - accessed May 19, 2015

<sup>54</sup> Ibid, Council of Europe (2015)

<sup>55</sup> Ibid., Council of Europe (2015)

the Directorate General of Human Rights and Rule of Law for the Council of Europe outlines the "*in concreto*" vs "*in abstracto*" issues underlying the dual criminality criteria. The first defines the act as being criminal while the latter outlines that the act may be punishable but not necessarily criminal<sup>56</sup>, therefore if two countries do not have the same meaning of criminality for the same act, then the decision usually falls onto the recipient of the request.

- Article 35 - 24/7 Network, requires the signatories of this convention to set up a type of 'hotline' whereby members can contact another in case of emergency - when immediate assistance and action is required. This requirement was inspired by a similar G8 subgroup that had a High-tech Crime network set up in 1997<sup>57</sup>. A study conducted by the Economic Crime division of the Council of Europe in 2007 indicated that most of the requests made through this network were deemed non urgent, while other requests were made through other existing and older channels - this brings into question as to whether the signatories should possibly set up an infrastructure that will allow for a central processing agency for mutual legal assistance so as to increase its efficiency. If the recipient of a request is ignorant of the fact that this 24/7 network existed for fighting cybercrime, then the information or assistance required may not be expedited to the right person in a timely manner<sup>58</sup>, which defeats the whole purpose of the network.

<sup>56</sup> Council of Europe (2015), "[http://www.coe.int/t/dghl/standardsetting/pc-oc/PCOC\\_documents/PC-OC%20%282012%29%202%20Final%20Note%20on%20dual%20criminality%20in%20concreto%20or%20in%20abstracto.pdf](http://www.coe.int/t/dghl/standardsetting/pc-oc/PCOC_documents/PC-OC%20%282012%29%202%20Final%20Note%20on%20dual%20criminality%20in%20concreto%20or%20in%20abstracto.pdf)" - accessed June 14, 2015

<sup>57</sup> Council of Europe (2015), "[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpoc\\_EN.asp](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpoc_EN.asp)" - accessed June 14, 2015

<sup>58</sup> Council of Europe (2015), "The functioning of 24/7 points of contact for cybercrime" discussion paper Prepared by the Economic Crime Division, April 2, 2009, pages 34-35  
[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/567\\_24\\_7report4public\\_april09a.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/567_24_7report4public_april09a.pdf) accessed June 14, 2015

## 6. ROLE OF AN IFA

Traditionally, IFA, as experts in financial matters, are engaged in business insurance claims, location of hidden assets and untangling of complex transactions when fraud is suspected.

However, a forensic accountant's role is not limited to fraud as they also have a good working knowledge of the legal system and aid in other litigation support engagements.<sup>59</sup> The role of an IFA is first and foremost to aid the Trier of fact - be it a court judge, jury, arbitrator or mediator, understand the underlying transactions at dispute as experts. Most recently, the use of IFAs can be seen in the Canadian news, relating to the investigation of several Senators expense claims and whether those claims complied with the rules that were set out - the result of these investigations yielded only a compliance report as the final determination of whether those claims were fraudulent is a matter for the Courts to decide.

The cost of engaging an IFA is usually quite high as the standards require them to consider all avenues, so as to show objectivity, and the required level of burden of proof that has to be obtained must meet the court's criminal code threshold of beyond a reasonable doubt as the IFA must always work under the assumption that their report might be used to prosecute someone. This also means that the evidence that is gathered during an IFA investigation must meet the court's criteria for admissibility as being relevant, reliable and non privileged. For evidence to be reliable, there must not be any tampering with the originals, and in an era where most of the records are kept in a digital format, the use of forensic computer experts is essential.

---

<sup>59</sup> Crumbley, D. L. (2011). *Forensic and Investigative Accounting* (5th Edition). Chicago, Illinois: CCH Incorporated, pp. 1-3 to 1-5.

In this new era of cybercrime the amount of information that any investigator must deal with is exponential - there are elements that can be used and deciphered by computer experts, but these experts may lack the financial or legal knowledge to determine whether the extracted information is relevant to the investigation. Therefore the need for a multi-disciplinarian expert or group working cohesively at the forefront or as the contact person for the Cyber Convention's 24/7 Network is highlighted and the IFA can play a role if one of these groups.

The changing landscape in the fight against money laundering and online fraud has created opportunities that the IFA can explore and those opportunities will be introduced in relation to recent news events.

### **A. Compliance monitor for MSP**

In a landmark case, the State of Arizona brought Western Union to court for not having enough controls in place to fight money laundering and knowingly not complying with United States anti-money laundering (AML) regulations after a Federal Trade Commission (FTC) investigation. The lawsuit was settled in 2010 and Western Union has agreed to settle for \$94 million dollars in payouts to the various states, funding an AML alliance (Southwest Border "SWB"<sup>60</sup>) and submit to a compulsory monitoring program for AML compliance for forty-one (41) months<sup>61</sup>. Western Union failed to implement all the recommendations stipulated by the

---

<sup>60</sup> Southwest Border Anti-Money Laundering Alliance (2015), "<http://www.swballiance.org/about-us/>" - accessed June 15, 2015

<sup>61</sup> Arizona Attorney General (2015), "<https://www.azag.gov/sites/default/files/sites/all/docs/swbamla/State%20of%20Arizona%20v.%20Western%20Union%20Settlement%20Agreement%20compact.pdf>" - accessed June 15, 2015

monitor as there were not enough controls set in place and the monitoring program has been extended to 2017.<sup>62</sup>

One of the role of the Monitor is to regularly evaluate the controls in place in order to determine on a risk basis whether certain transactions should have been flagged as suspicious and compare it to the SWB's assessment of these same transactions. These controls that are to be set up can be at the entry level, ie the clerks, or at a programming level, where patterns are to be detected and then on a supervisory level where an experienced analyst can review both sets of controls. There is an opportunity here for the IFA to work at the supervisory level as they have the financial experience and professional skepticism that may allow them to discern patterns better than a program can, as some transactions may be flagged as suspicious but are not; and for compliance purposes, they can ensure that the documentation required to deny or support a case of money laundering is properly included and should be part of the Western Union's AML controls on a ongoing basis.

MoneyGram is the second largest MSP, after Western Union, was recently fined \$100 million for flagrantly ignoring the complaints of over 19,000 instances between 2004-2008 in the United States and Canada, despite having an internal fraud department that had outlined several employees that they believed were involved in fraud schemes.<sup>63</sup> An enhanced monitoring for compliance obligations required the "creation of an independent compliance and ethics committee of the board of directors with direct oversight of the chief compliance officer and the

---

<sup>62</sup> Ensign, R. L., "Western Union Faces More Scrutiny Over Money Laundering Controls", Wall Street Journal, February 3, 2014, "<http://www.wsj.com/articles/SB10001424052702304626804579361274287589350>" - accessed June 15, 2015

<sup>63</sup> KriebsonSecurity (2012, November), "<http://kriebsonsecurity.com/2012/11/moneygram-fined-100-million-for-wire-fraud/>" - accessed June 15, 2015



compliance program"<sup>64</sup>. For the same reasons stated above, an IFA with the relevant expertise would be able to add to the oversight function of the compliance program required.

It is important to note here that to maintain the integrity of the IFA profession, the threat of familiarity and perceived lack of objectivity needs to be considered when taking on these engagements on a repeat basis.

### **B. Disruption program analyst**

The Australian Competition & Consumer Commission (ACCC) recently released results from their 2014 scam disruption project with AUSTRAC (Australia's FINTRAC counterpart) and the banking industry in identifying potential victims of scams. The agents involved in the project reviewed banking activities and identified those transactions that may be unusual in the sense that they may have been as a result of fraud, with an emphasis on romance scams. The individuals were then contacted via regular post and over 70 percent of those who received a letter stopped sending money overseas immediately.<sup>65</sup>

The immediate impact of the project shows the real potential that can be achieved through the analysis of the client's banking activities and is an area that an IFA could assist as experts in determining the reasonability of certain transactions through the review of historical patterns, lifestyle and business purposes. The disruption programs in Canada have not reached this level

---

<sup>64</sup> "<http://www.justice.gov/opa/pr/moneygram-international-inc-admits-anti-money-laundering-and-wire-fraud-violations-forfeits>" - accessed June 15, 2015

<sup>65</sup> ACCC (2015), "Targeting Scams - Report of the ACCC on scams activity 2014, May 2015, page 19

but there are privacy issues that have to be considered and the IFA, being well-versed in the legal system should be able to navigate the changing landscape.

The goal of these disruption programs is to make it more difficult for the scammers to achieve their goal - money from their victims. The collaboration with the banking industry educates not only the potential victims, who may not be aware that they are being scammed, but also the clerks that are at the forefront and have a large role in deterring the victims from sending the money. MSP clerks also have the same role in deterring potential victims from sending money to people they have never met, but it is not a practice that is enforced in every branch, as evidenced by the MoneyGram settlement.

With government agencies cracking down on MSP, the scammers are using other methods to try to get their funds. The following ones are becoming more popular as they are easy to use:

- The use of prepaid credit cards purchased within Canada is usually not flagged to be monitored and the cards can be sent overseas or the numbers can be communicated to the scammers.
- There is an increase in "electronic cash" services (e-cash) where the virtual currency can be purchased at various gas stations or the post office and the numbers are forwarded to the scammers overseas to be redeemed on websites that accept these payment methods.

The ease of use is two-fold: the victims do not need to have any knowledge in how to procure these payment methods other than to ask it from the clerk and they can be bought with cash.

There is no current requirement for these entities to report the sale of these alternative cash

methods but if their use increases, then there might come a day when reporting will be made mandatory and there might be a role for an IFA.

### **C. Online dating fraud detection**

Due to the large number of victims meeting their scammers through online dating websites, a few class action lawsuits have been filed against different dating websites. Match.com being the largest player in the United States had been named in several suits and most recently for having fake profiles in which stolen pictures were being used<sup>66</sup>. They have officially stated that the company has "an extensive fraud management team comprised of certified fraud examiners (CFE), analysts and technologists who police all entry point for fraud - and review users who meet a basic threshold of risk".<sup>67</sup> The investigative experience that CFE and IFA develop over their professional career are similar, therefore the role can be filled by an IFA as well.

When the characteristics of the scammers are all befuddled by social engineering and the tracking of internet activity can be masked by software the only concrete thing that law enforcement can trace is the money trail and the experienced IFA would have the skills to do so.

---

<sup>66</sup> Fagenson, Z. "Romance website Match.com sued for \$1.5 billion over 'unauthorized' photos", Reuters November 25, 2013, "<http://www.reuters.com/article/2013/11/25/usa-florida-match-idUSL2N0JA1DJ20131125>" - accessed May 16, 2015

<sup>67</sup> Ibid Quinn, J., The Star (2013)

## 7. FUTURE FRAUD TENDENCIES

The internet has seemingly created the need for individuals to constantly stay in touch through social media and the integration of the computer into an older standard, the telephone, has brought the scammers back full circle. The availability of voice-over-internet-protocol (VOIP) and software that allows the fraudster to mask their phone numbers have increased the risk of victims to paying out or divulging confidential information, while decreasing the operational cost for scammers.

The number of potential victims that can be reached by telephone is still larger than those on the computer as there still exists a resistance to that technology but virtually everyone has a phone or two. The chances that those who have a reticence against computers are not enlightened of all the existing scams, and the technologies that facilitate it, and thus more vulnerable to falling for the fraudster's traps.

The use of "robocalls", having computers dial a generated list of numbers with a pre-recorded message and then when a connection is made with an actual person the scammers will interact with the potential victims to try to extract the required information, allows for thousands of calls to be made on a daily basis at a very low cost. The speed with which these scams have taken off in the last month has required just as swift a reaction from the legitimate businesses that were being impersonated - see Appendix B.

All in all, the types of fraud that are the most effective have not changed at its core, it's just the delivery method and the mode of receiving the wares that have evolved making it predictable but not necessarily preventable as human nature is not always rational.

## CONCLUSION

Fraud will always be evolving as the scammers adapt newer technology at a faster rate and understands the opportunities that are presented better than regular users and those charged with protecting them. Because of all the different permutations any one scam can present itself, it is important to educate the public of the ever present risk of being defrauded and to recognize the red flags before suffering more losses. There is also a required attitude change that must come as a result of the continuous education of the general public and the law enforcement officers - everyone is vulnerable and can become a victim: blame and shame should not be assigned to those who have suffered losses as they will continue to remain silent.

The transnational aspect of dot-cons stresses the need for international cooperation and law enforcement entities in the countries that have the highest number of victims have recognized the growing dangers that the internet presents and are trying to deter the scammers

- by imposing harsher sentences (US extradition instances have increased and enhancement sentences for vulnerable victims),
- making it harder to obtain funds by imposing and enforcing AML controls on all financial entities; and
- educating the public in general of the risks and the signs that they or someone they know are being defrauded.

The criticism that the sentences do not reflect the crime is especially telling in instances where several fraudster work together to potentially defraud millions from multiple individuals - the

role of the IFA in this instance would be more traditional, ie the tracing of funds and untangling the comingled funds would be important in illustrating the gravity of the economic losses suffered at their hands. All the potential roles for IFAs in this new era of online scams involve an element of prevention - the investigative skills, professional skepticism and legal knowledge that the IFA possess allows them to aid in the location of potential victims and the location of assets for restitution possibilities.

As the popular adage goes, "an ounce of prevention is worth a pound of cure" - the future of the IFA profession could very well have a larger impact outside of the courts than it ever had in the past.

## APPENDIX A - EXAMPLES OF DOT-CON

### 1. Advance fee - job offers

**From:** serche Dremil <[serche31@outlook.fr](mailto:serche31@outlook.fr)>  
**Date:** May 7, 2015 at 6:12:59 PM GMT-4  
**To:** [REDACTED]  
**Subject:** Job Offer (/3180<Fwn17)

Hi,

Our famous firm is an international brand in the financial market. We commenced our business in the US. But nowadays we doing business in various countries. Just now we doing business in Canada.

Let us to tell you, that our company is interested in you for the Financial Assistant post. Due to the firm's enlargement and breaking into the new sectors, we are glad to give you an opportunity to become a part of our ambitious team.

Please, look at our offer:

Job title: Financial Assistant;  
Country: Canada;  
Pay rate: \$5200-\$10000 CAD/month;  
Suitable work schedule;

Main requirements for the Financial Assistant position:

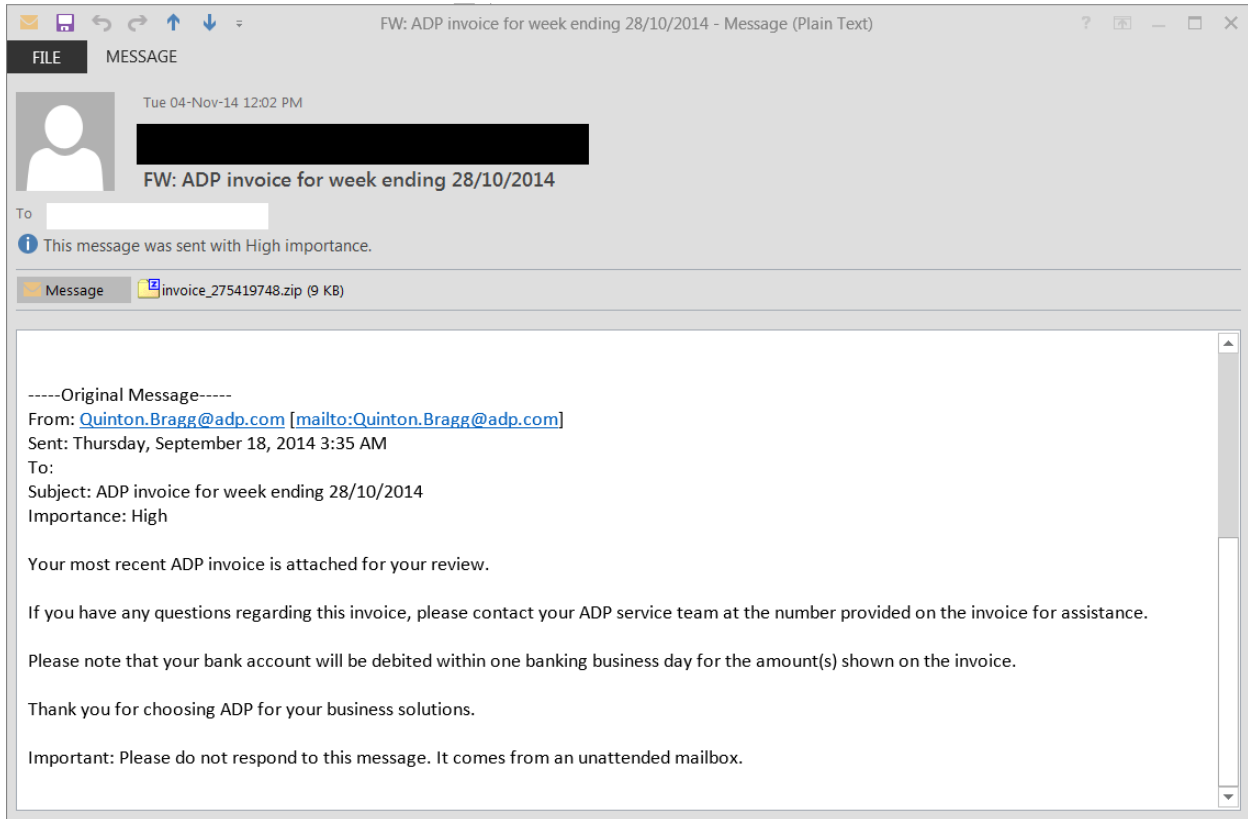
Resident of Canada;  
18+;  
Internet access;  
Mobile phone communication;

For enquiries, please reply us at: [gatarika1971@mail.com](mailto:gatarika1971@mail.com) .  
Your Resume will be a great plus for our decision.

We are looking forward to your early reply.



## 2. False Invoice with malware



The screenshot shows an email client window titled "FW: ADP invoice for week ending 28/10/2014 - Message (Plain Text)". The window has a "FILE" menu and "MESSAGE" title bar. The email header shows a sender profile icon, the date "Tue 04-Nov-14 12:02 PM", and the subject "FW: ADP invoice for week ending 28/10/2014". The recipient field is redacted. A notification states "This message was sent with High importance." The attachment bar shows "Message" and "invoice\_275419748.zip (9 KB)". The main content area displays the original message text:

-----Original Message-----  
From: [Quinton.Bragg@adp.com](mailto:Quinton.Bragg@adp.com) [<mailto:Quinton.Bragg@adp.com>]  
Sent: Thursday, September 18, 2014 3:35 AM  
To:  
Subject: ADP invoice for week ending 28/10/2014  
Importance: High

Your most recent ADP invoice is attached for your review.

If you have any questions regarding this invoice, please contact your ADP service team at the number provided on the invoice for assistance.

Please note that your bank account will be debited within one banking business day for the amount(s) shown on the invoice.

Thank you for choosing ADP for your business solutions.

Important: Please do not respond to this message. It comes from an unattended mailbox.

### 3. Inheritance scam

**From:** Mr. Jonathan David <postmaster@imangement.com.br>  
**Sent:** Friday, April 03, 2015 7:06 PM  
**Subject:** Re:Contact the verification officer incharge of the delivery:

*Dear Beneficiary,*

*This is to officially inform you that we have written to you before without getting respond from you and we believe that our previous mail did not get to you therefore we write you again. We are contacting you concerning the release of your inheritance fund / Draft /Cheque /ATM Card which have been delayed for transfer by some officials who claim to be in position of your fund thereby extorting money from you in one way or the other.*

*Your Fund has finally been approved for transfer by the West Africa Fund Monitoring Unit. Your fund will be transfer to you via MasterCard ATM which is cashable in any ATM machine or Bank anywhere in the world.*

*We hereby inform you that the ATM card worth US\$8.5, 000.000.00 has been credited in your favour as the first part payment of your inheritance fund which has been delayed by these officers who claim to be in position of your fund.*

*Therefore you are warned to stop any further communication with anybody concerning your inheritance fund.*

*Your fund to be released via MasterCard ATM in act to uphold the rule of law which we represent. You have to reconfirm the informations below for security reasons. The only money you are obliged to pay is the delivery charges only .*

*Contact the verification officer incharge of the delivery:*

*Name: Mr. Jonathan David  
E-mail: atm.card15@yandex.com  
Telephone +2348034121432*

*Send them the following informations of yours for the conclusion of your ATM Card:*

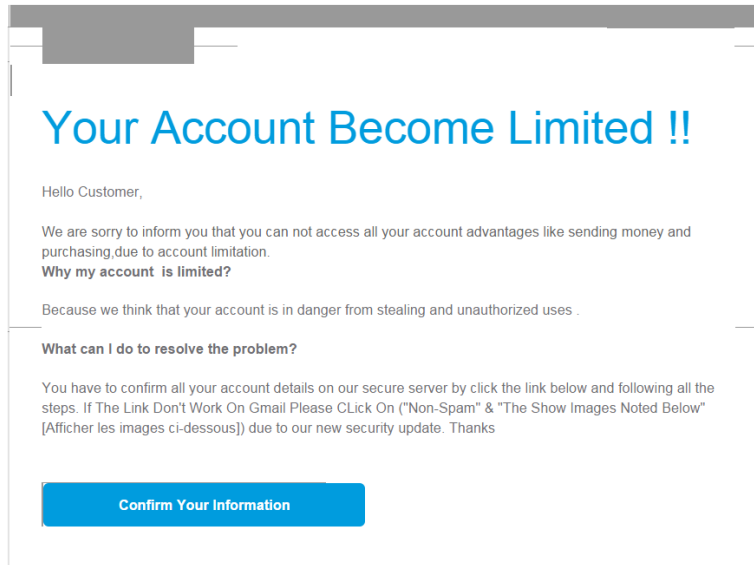
*Full Name: \_\_\_\_\_*

## 4. Phishing email

Your PayPal account has been limited until we hear from you (Case ID #PP-003-498-237-832)

↑ ↓ ✕

Parts of this message have been blocked for your safety.  
[Show content](#) | [I trust service@intl.paypal.com](mailto:trust.service@intl.paypal.com). Always show content.



## APPENDIX B - COMPANY REACTION



Dear

Hilton Worldwide recently became aware of a fraudulent, organized campaign of telemarketing "robocalls" that appears to target Canadian residents. The call recipients are asked to provide personal information, including credit card information to receive free nights at a major hotel provider.

We want to make it clear that these calls are not originating from Hilton Worldwide and have no validity. If anyone receives such a call, they should hang up and not provide any sensitive or personal information.

We take information security very seriously and have notified the appropriate law enforcement authorities. More information on telephone scams can be found on the Canadian Telecommunications Commission's Web site: [http://www.crtc.gc.ca/eng/info\\_sht/g9.htm](http://www.crtc.gc.ca/eng/info_sht/g9.htm).

We value your privacy; under no circumstance will we contact you to request personal or credit card information. We only request these details when a guest books a reservation or promotional package by telephone, and we will never ask for your HHonors account log-in details. If you receive any such a



## BIBLIOGRAPHY

Arizona Attorney General (2015) settlement with Western Union

"<https://www.azag.gov/sites/default/files/sites/all/docs/swbamla/State%20of%20Arizona%20v.%20Western%20Union%20Settlement%20Agreement%20compact.pdf>"

Better Business Bureau

"<http://www.bbb.org/mbc/news-centre/news-releases/2014/02/2014-top-ten-scams/>"  
accessed on May 5, 2015

Buse, U. "Spam Scams: Africa's city of cyber gangsters", November 7, 2005, Spiegel International

"<http://www.spiegel.de/international/spiegel/spam-scams-africa-s-city-of-cyber-gangsters-a-384317.html>" - accessed May 2, 2015

CBC News (2013, January 15)

"<http://www.cbc.ca/news/canada/british-columbia/top-10-scams-of-2013-1.1328875>"  
accessed on May 5, 2015

CBC News (2013, September 30)

"<http://www.cbc.ca/news/canada/british-columbia/man-duped-500k-in-online-romance-scam-1.1870043>" - accessed May 5, 2015

Canadian Anti-Fraud Center (CAFC)

"<http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/types/romance-rencontre/index-eng.htm>" accessed on June 3, 2015

Canadian Anti-Fraud Center (CAFC)

"<http://www.antifraudcentre-centreantifraude.ca/english/stopit-faq/html>" - accessed April 7, 2015

Canadian Anti-Fraud Center (CAFC)

"<http://www.antifraudcentre-centreantifraude.ca/about-ausujet/index-eng.htm>" - accessed June 13, 2015

### Competition Bureau

"<http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03074.html>" accessed on May 5, 2015

### Council of Europe (2015)

"<https://www.europol.europa.eu/faq#n77>" - accessed May 19, 2015

### Council of Europe (2015)

<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> - accessed May 19, 2015

### Council of Europe (2015)

"[http://www.coe.int/t/dghl/standardsetting/pc-oc/PCOC\\_documents/PC-OC%20%282012%29%202%20Final%20Note%20on%20dual%20criminality%20in%20concreto%20or%20in%20abstracto.pdf](http://www.coe.int/t/dghl/standardsetting/pc-oc/PCOC_documents/PC-OC%20%282012%29%202%20Final%20Note%20on%20dual%20criminality%20in%20concreto%20or%20in%20abstracto.pdf)" - accessed June 14, 2015

### Council of Europe (2015)

"[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpoc\\_EN.asp](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpoc_EN.asp)" - accessed June 14, 2015

### Council of Europe (2015)

"The functioning of 24/7 points of contact for cybercrime" discussion paper Prepared by the Economic Crime Division, April 2, 2009, pages 34-35

### Council of Europe (2015)

"[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/567\\_24\\_7report4public\\_april09a.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/567_24_7report4public_april09a.pdf)" accessed June 14, 2015

Corey Janssen "<http://www.techopedia.com/definition/23397/dot-con>" - accessed on April 7, 2015

Crumbley, D. L. (2011). *Forensic and Investigative Accounting (5th Edition)*. Chicago, Illinois: CCH Incorporated

### Egmont Group

Egmont Group of Financial Intelligence Units, Annual Report 2012-2013

### Egmont Group

An Egmont Group White Paper - "The Role of Financial Intelligence Units in Fighting Corruption and Recovering Stolen Assets", September 2012

Ensign, R. L., "Western Union Faces More Scrutiny Over Money Laundering Controls", February 3, 2014, Wall Street Journal  
"<http://www.wsj.com/articles/SB10001424052702304626804579361274287589350>" - accessed June 15, 2015

### Europol

THE INTERNET ORGANISED CRIME THREAT ASSESSMENT (iOCTA) 2014  
"<https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta>" - accessed May 20, 2015

### Europol

Europol June 2010 Threat Assessment  
"[http://www.fincen.gov/news\\_room/rp/reports/pdf/IMMFTAFinal.pdf](http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf)" - accessed May 20, 2015

### Europol

Europol, Threat Assessment (Abridged)- Internet facilitated organized crime (iOCTA) July 2011

Fagenson, Zachery "Romance website Match.com sued for \$1.5 billion over 'unauthorized' photos, Reuters November 25, 2013 "  
"<http://www.reuters.com/article/2013/11/25/usa-florida-match-idUSL2N0JA1DJ20131125>" - accessed May 16, 2015

Fumano, D. "Con man 'could talk the fleas off a dog' but he's messed with the wrong girl", July 5, 2013, The Province  
"[http://www.theprovince.com/story\\_print.html?id=8612967&sponsor=escapes.ca](http://www.theprovince.com/story_print.html?id=8612967&sponsor=escapes.ca)" - accessed May2, 2015

Government of Canada - Fact sheet: Privacy Protection and the Protecting Canadians from Online Crime Act

"<http://news.gc.ca/web/article-en.do?ctr.sj1D=&ctr.mnthndVl=11&mthd=advSrch&ctr.dpt1D=6681&nid=832379&ctr.lc1D=&ctr.tp1D=&ctr.yrStrtVl=2013&ctr.kw=&ctr.dyStrtVl=3&ctr.aud1D=&ctr.mnthStrtVl=11&ctr.page=1&ctr.yrndVl=2013&ctr.dyndVl=29>" - accessed June 13, 2015

Government of Canada

"<http://www.getcybersafe.gc.ca/cnt/cbrblng/prnts/lgl-cnsqncs-en.aspx#a02>" - accessed June 13, 2015

Hicken, M, "I was a victim of an online dating scam" February 20, 2013, CNN Money,

"<http://money.cnn.com/2013/02/20/pf/online-dating-scam/>" - accessed May 24, 2015

INTERPOL (2015)

"<http://www.interpol.int/Crime-areas/Financial-crime/Fraud/419-fraud>" - accessed June 5, 2015

INTERPOL (2015)

"<http://www.interpol.int/About-INTERPOL/Funding>" - accessed June 5, 2015

INTERPOL (2015)

"<http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>" - accessed June 5, 2015

INTERPOL (2015)

"<http://www.interpol.int/Crime-areas/Cybercrime/Operations>" - accessed June 5, 2015

INTERPOL (2015)

"<http://www.interpol.int/News-and-media/News/2014/N2014-228>" - accessed June 5, 2015



Johnson, M. A. "Older women most likely to click with online romance scam artists" May 14, 2013, NBC News

"[http://usnews.nbcnews.com/\\_news/2013/05/14/18255848-older-women-most-likely-to-click-with-online-romance-scam-artists?lite](http://usnews.nbcnews.com/_news/2013/05/14/18255848-older-women-most-likely-to-click-with-online-romance-scam-artists?lite)" - accessed May 15, 2015

Karen H., Confidence Men and Painted Women, Yale University Press, 1982

KrebsonSecurity.com

"<http://krebsonsecurity.com/2012/11/moneygram-fined-100-million-for-wire-fraud/>" - accessed June 15, 2015

Merriam Webster dictionary (2015)

"<http://www.merriam-webster.com/thesaurus/confidence%20man>" accessed on June 2, 2015

Merriam Webster dictionary (2015)

"<http://www.merriam-webster.com/dictionary/scam>" accessed on June 3, 2015

Oxford Dictionary

<http://www.oxforddictionaries.com/definition/english/conman> accessed on June 2, 2015

National Crime Agency (2015)

"<http://www.nationalcrimeagency.gov.uk/news/news-listings/478-romance-fraud-mastermind-jailed-in-ghana>" - June 15, 2015

Power, J., "Love me don't: the West African online scam using US soldiers", December 6, 2014 from The Sydney Morning Herald

"<http://www.smh.com.au/good-weekend/love-me-dont-the-west-african-online-scam-using-us-soldiers-20141204-11szid.html>" - accessed May 14, 2015

Public Prosecution Service of Canada

"<http://www.ppsc-sppc.gc.ca/eng/pub/fpsd-sfpg/fps-sfp/fpd/ch43.html#section43>" - accessed June 13, 2015

Quinn, J. "Online dating relationship ends badly, \$1.3M later", November 30, 2013, The Star

"[http://www.thestar.com/news/world/2014/02/06/the\\_cost\\_of\\_love\\_alleged\\_fraudster\\_leaves\\_broken\\_hearts\\_empty\\_bank\\_accounts.html](http://www.thestar.com/news/world/2014/02/06/the_cost_of_love_alleged_fraudster_leaves_broken_hearts_empty_bank_accounts.html)" - accessed May 15, 2015

Shadel, D. and Dudley, D., "Are you real? - Inside an Online Dating Scam" AARP Magazine, June/July 2015  
"<http://www.aarp.org/money/scams-fraud/info-2015/online-dating-scam.html>" - accessed June 13, 2015

Simpson, C. "Scammers took \$89 Million from Australians in 2013" June 16, 2014  
"<http://www.gizmodo.com.au/2014/06/scammers-took-89-million-from-australians-in-2013/>" - accessed June 4, 2015

Southwest Border Anti-money Laundering Alliance (2015)  
"<http://www.swballiance.org/about-us/>"

Stevens, C., "Online romance scams bilk Canadians out of nearly \$14M in 2014", March 9, 2015, Global News  
"<http://globalnews.ca/news/1873036/online-romance-scams-bilk-canadians-out-of-nearly-14m-in-2014/>" - accessed May 31, 2015

Sydney Criminal Lawyers blog  
"<http://www.criminallaw.com.au/blog/criminal/general/online-love-predators-raking-in-millions/35323>" - accessed June 4, 2015

United States Justice Department  
"<http://www.justice.gov/opa/pr/moneygram-international-inc-admits-anti-money-laundering-and-wire-fraud-violations-forfeits>" - accessed June 15, 2015

Whitty, M. "The Psychology of the Online Dating Romance Scam" - April 2012"  
"<http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/02775.html>" - accessed May 15, 2015