Article

ANZSOC

Australian & New Zealand Journal of Criminology
2020, Vol. 53(4) 497–514

DOI: 10.1177/0004865820957077
journals.sagepub.com/home/anj
SAGE

Understanding pet scams: A case study of advance fee and non-delivery fraud using victims' accounts

Jack M Whittaker
Department of Sociology, University of Surrey, UK

Mark Button
Institute of Criminal Justice Studies, University of Portsmouth, UK

Abstract

Advance fee and non-delivery frauds have become very common with the growing preference for online shopping and the new opportunities this brings for online offenders. This article uses unique access to a volunteer group's database focused on preventing pet scams to explore this type of crime. Distances, among other factors, make the purchase of pets online common in countries such as the USA, Australia and South Africa. This modality of purchase has been exploited by organized criminals largely based in Cameroon to conduct advance fee and non-delivery frauds. The article uses data from the volunteer group Petscams.com to provide unique insights on the techniques of the offenders with particular reference to the strategies used to maximize victimization by using real accounts of victims of such frauds. It also briefly notes how the COVID-19 crisis has been used to adapt this type of scam. The article's discussion identifies the need for a more nuanced assessment into the role of victim oriented voluntary organizations.

Keywords

Cybercrime, fraud, pet scams, scams, techniques

Date received: 12 May 2020; accepted: 17 August 2020

Corresponding author:
Jack Whittaker, Department of Sociology, University of Surrey, Surrey GU2 7XH, UK.
Email: jackmwhittaker@gmail.com

Introduction

The global cybercrime economy has co-existed alongside the digital economy since its inception and is currently estimated to be worth at least an estimated $1.5 trillion per year (Mcguire, 2018). Scholars have identified that a key component of this lucrative economy is 'platform crime', the incorporation of online platforms into criminal modalities (Levi, 2016; Mcguire, 2018). Cybercriminals may seek to exploit existing platforms created for legitimate purposes for a variety of online crimes such as credit card phishing, cyberstalking and to spread malware (Button & Cross, 2017; Cross, 2015; Prenzler, 2017; Soomro & Hussain, 2019; Van Wilsem, 2011). Platforms may also be tailor-made and commoditized for the purpose of providing cybercriminals with means to access a plethora of online tools in what has been defined as 'cybercrime-as-a-service' (Mcguire, 2018). The rise in these personalized cybercrime platforms provides online offenders with unprecedented access to illegal products and services such as botnet rentals, virus infection services and crimeware upgrade models in what is becoming an increasingly sophisticated and specialized black market (Ablon & Libicki, 2015; Manky, 2013). The definition of a cybercrime-as-a-service platform lies in its malicious output, whether that is to perform a Distributed Denial of Service Attack attack against a target's computer, phish for credit card information through targeted emails or to infect a computer with viruses and malware.

This article will provide a qualitative study of victim complaints made to an online volunteer anti-fraud organization to demonstrate that non-malicious websites have been integrated into non-delivery fraud, a specific modality of advance fee fraud whereby online offenders attempt to defraud consumers purchasing products on the internet. Non-delivery fraud exploits the growth in online shopping which is estimated to be at its highest recorded levels. Consumers were expected to have spent $3.46 trillion in the global online marketplace in 2019, an increase of over 18% from 2018 according to Internet Retailer (Young, 2019). This study of non-delivery fraud seeks to identify that the websites used by online offenders are malignant in terms of their functionality as static web 2.0 platforms, akin to the millions of other legitimate websites available on the internet, but instead provide a useful platform to assist their social engineering efforts against potential victims. It will begin by placing non-delivery fraud within the context of cyberfraud before identifying the opportunities for offenders to exploit the enhanced vulnerability which consumers are exposed to when shopping online. The methodology will then outline how a desk-based approach was taken to retrieve and catalogue victim complaints from a voluntary consumer-focused organization called petscams.com which specializes in warning victims about the threat of fraudulent pet websites. The results of the investigation will identify the most popular animal species and breeds used in pet scams. It will also provide a qualitative analysis to demonstrate how offenders extort initial pet deposit payments and multiple recurring secondary fees from victims. The conclusion discusses the implications of this study for routine activities theory and suggests further research avenues by focusing on the role of voluntary organizations in preventing fraud.

Cybercrime and non-delivery fraud

It is widely acknowledged that cybercrime evolves and adapts at a rapid pace in a continuing arms race between the illicit underground demand for products which

facilitate cybercrime and tools to counter the threats that they pose to governments, businesses and the wider public (Boddy, 2018; Chouhan, 2014; Kraemer-Mbula et al., 2013). Advance fee fraud is one such example of a technology crime that has undergone a substantial evolution from its origins in 419-email scams which emerged in Nigeria during the 1990's when offenders sought to proposition internet users with offers of million-dollar lottery wins, business propositions and trunk boxes containing gold (Ampratwum, 2009; Dion, 2010; Durkin & Brinkman, 2009; Holt & Graves, 2007). The practice of using confidence tricks to elicit advance fee payments has subsequently spread to neighbouring West African countries. Offenders located in neighbouring countries such as Benin, Cameroon and Ghana have sought to place their own hallmarks on advance fee fraud by producing newer and more sophisticated ways in which internet users can been defrauded. Some notable examples of this evolution include but are not limited to business–email–compromise, romance fraud and the non-delivery of products ordered online (Better Business Bureau, 2017; Mansfield-Devine, 2016; Sorell & Whitty, 2019; Whitty, 2015).

The Better Business Bureau, a US based non-profit organization which promotes marketplace trust between consumers and businesses, commissioned a 'Scam Study' report on the non-delivery of pets in 2017 and identified that there is a flourishing consumer fraud economy for products that do not exist. The study found that up to 80% of all sponsored advertising links on the internet are estimated to be promoting fraudulent websites which have been created by offenders located in Cameroon (Better Business Bureau, 2017). The popularity of internet fraud in Cameroon has also been explored by Abia et al. (2010) which surveyed 300 students to determine how well fraud is understood by students. The survey identified from a sample of 300 Cameroonian students that 91% of participants were aware of internet fraud and that of this figure 53% were informed by friends, of whom 15% were themselves actively participating in internet fraud.

The use of online environments in advance fee fraud is particularly advantageous for offenders and poses a significant difficulty for law enforcement efforts. Offenders can be located anywhere in the world, often in the poorest and most disadvantaged countries, and will never come into physical contact with their victims (Button et al., 2014). Furthermore, offenders can easily hide their location by using virtual private networks and seek to create anonymous or falsified online identities (Webster & Drew, 2017). Law enforcement efforts have in many cases responded by introducing new and specialist initiatives to investigate and tackle the threat of cybercrime. The Australian Cyber Security Centre for example is the Australian government's response to cybercrime and encourages victims of these crimes to submit a report through its cybercrime reporting facility known as ReportCyber. The Federal Bureau of Investigation (FBI) has also introduced a similar initiative for US citizens called the Internet Crime Complaint Center (IC3). The initiative provides US citizens with a reporting mechanism to submit information concerning suspected internet facilitated criminal activity. Voluntary policing initiatives have also entered the fray in what has been coined as 'digilanteism' (Button, 2019, 2020). Organizations such as petscams.com have created their own online repositories of fake websites and provide access of these data to law enforcement, government agencies and researchers.

Pet scams

This paper will use the example of pet scams of which there has been very little research to date. The essence of these scams is the advertisement of a pet such as a dog or cat online with the purpose of enticing victims to make an advance fee deposit for pets and an array of other associated costs such as for the delivery of the animal. This is a distinctly separate issue to animal related welfare practices such as puppy farms and cases of illness, genetic inbreeding or malnutrition which are discovered upon receipt by the buyer. The fraud examined in this paper examines cases when an offender intends to collect payments for a pet despite having no intention of delivering it to the buyer.

In countries such as the USA, Australia and South Africa because of their large geographical size, it is common to purchase pets online. In the UK, by contrast, it is usually quite feasible to drive to a prospective seller's premises and view the pet before buying. In countries such as the USA and Australia, this is not always practical. For example, purchasing a pedigree dog from a dealer in Perth when the prospective owner lives in Sydney would be timely and costly to do it in person. Thus, the online advertisement of pets has become quite common in such countries with prospective owners viewing pets online, purchasing them and paying for them to be shipped to the home address. This method of online shopping for pets has created substantial new criminal opportunities, which will be the focus of the rest of this paper.

Consumer vulnerability and cybercrime

Several factors have been attributed to the motivations for the increase in online shopping: first and foremost is the enhanced convenience which enables consumers to place online orders at the click of a mouse without having to visit a traditional bricks and mortar store (Rohm & Swaminathan, 2004; Swaminathan & Lepowska-White, 1999). A second motivation is that consumers are able to search, compare and access information of products with greater ease and depth than with traditional stores (Alba et al., 1997; Lynch & Ariely, 2000; Rohm & Swaminathan, 2004). One particular problem which can be attributed to this is that consumers are not able to physically see or touch their product until after the purchase has taken place and the product has been delivered. Consumers who seek the benefits derived from the immediate possession of a product therefore may instead choose to shop within a traditional bricks and mortar store (Rohm & Swaminathan, 2004; Shaw, 1994; Sheth, 1983). For those consumers which choose to ignore the many product and company review websites available online, they subsequently become at a higher risk of being exposed to opportunistic cybercriminals which have sought to create a thriving online marketplace of deception and fraudulent practices. Malicious parties can register website domains with ease to create their own e-commerce websites for the sole purpose of taking advantage of the trust-based relationship in the online purchasing process between the buyer and seller.

Cybercriminals may seek to undermine the element of trust between buyer and seller by creating websites for the sale of counterfeit products to falsify or hijack brands through the illegal violation of copyright patents to distribute lower quality and cheaper products (Chaudhry & Stumpf, 2011). Malpractice can also take place through non-delivery Fraud which has been acknowledged as a particular problem for online auction

websites. In this type of fraud, an online offender will list a non-existent product for sale, receive payment for the goods and later disappear without any trace (Almendra, 2013; Van Wilsem, 2011). The FBI recorded in its 2019 IC3 report 61,832 complaints from victims of non-delivery fraud with accumulated losses totalling $196,563,497. The non-delivery of pets provides a particularly significant challenge for consumers. An internal report prepared by the Federal Trade Commission in 2015 identified some 37,000 complaints involving pets with the majority believed to be relating to non-delivery fraud (Better Business Bureau, 2017). This problem is not an isolated phenomenon in the USA. The Australian Competition and Consumer Commission's website Scamwatch reported consumer losses in the online purchase of pets amounting to $310,000 in a 12-month period ending March 2018 (Better Business Bureau, 2017).

Methodology

The data source for this research was the voluntary organization 'petscams.com' which maintains a database of approximately 18,000 fake pet and shipping websites used in non-delivery fraud. The organization is run by a small group of volunteers who seek to identify fraudulent pet websites on the internet and list each fraudulent pet website as an individual warning page. Their goal is to rank each warning page next to the corresponding fraudulent website on a potential victim's search engine results. The organization also encourages comments on these warning pages which are moderated by its volunteers to prevent offenders from seeking interaction with previous or potential victims.

The authors acknowledge that there are multiple other resources available to victims of pet scams where they may lodge their complaints to such as government agencies which collect victim complaints. Australian citizens for example can report instances of fraud to the Australian Competition and Consumer Commission whilst US citizens can report their own experiences to the FBI's IC3. The logic for using petscams.com as the data source for this study was based on the narrow scope of the victim complaints, which have in all cases been made by victims of non-delivery fraud. The fraudulent websites themselves were also considered for further analysis, however, it was quickly identified that in nearly all cases they were taken offline after complaints had been made to the organization.

A desk-based approach was taken to collecting the victim complaint comments made to the organization from the start of its comment archive database on 1 May 2017 to a cut-off date of 31 March 2020. During the initial data collection phase, the authors applied for formal access to the data and were granted access to the website's comment moderation panel which contained a centralized version of the comments from all of the warning pages. Access was granted on the basis of anonymizing any data used from analysis for publication purposes. The researchers did not seek access to contact any victims and as the research was based upon existing data collected by Petscams.com this meant that no ethical approval was required by the authors' universities.

In the first instance, data were collected when a monetary loss amount was specified by a complainant which resulted in the initial collection of 483 individual victim complaints for further analysis from a pool of 3119 total comments made to petscams.com during the data collection period. The collection of only monetary loss complaints in the

first stage allowed a high volume of irrelevant comments to be disregarded such as spam, irrelevant enquiries, ineligible complaints, duplicate complaints and complaints which were deemed to be too minimal in content for further analysis. The complaints were subsequently divided into two main categories: 415 complaints were identified as being made specifically against deposit payments placed on pets and a further 68 complaints were made against the costs associated with shipping after the initial deposit payment had been made. The 415 pet deposit complaints were then subsequently catalogued by breed and by monetary loss amount to identify popular animal species and breeds used in pet scams.

The complaint comments were then catalogued using thematic coding (Corbin & Strauss, 1990; Strauss, 1987). Complaints from both the initial deposit and shipping fees were placed into four distinct themes for further analysis. A first category was developed by identifying the primary motivations by the complainants for placing an initial pet deposit without conducting further due diligence. This first theme provided the researchers with valuable insight to explore both the level of professionalism employed in the creation of fraudulent websites and how the offenders initiated the trust-building process with the victims. A second category was developed based upon the authors' identification that many of the complainants were defrauded by several fictitious fees associated with the process of shipping a pet. The 68 complaint comments made against secondary shipping fees were catalogued by the numerous justifications used by the offenders for this process. It provided the authors with the opportunity to explore how the offenders intended to revictimize those victims which had already paid a pet deposit payment and how they were able to keep those victims hooked throughout the entire purchase process. A third category was developed by cataloguing the many payment methods used by the offenders for both the initial pet deposit payment and the shipping fees. This was to develop an understanding of how the offenders were laundering the stolen funds. The authors were particularly interested to identify whether money transfer platforms were still the most popular payment methods accepted in fraudulent purchases, which have been historically used in advance fee fraud practices to avoid currency transaction reports (Magnusson, 2009). A fourth category was developed by using the non-victim complaint comments to identify the primary justifications into why they had decided not to purchase their desired pet. The authors identified 156 comments from the remaining pool of 2636 comments which were instances when a complaint had been received but no monetary amount was lost by the complainant. These data were sorted into two main themes: that the fraudulent website used by the offender was not deemed by the complainant to be believable and that second there were irregularities in their communications with the offender which resulted in complainants backing out of the purchase process. This provided the authors with insight into how some due diligence was conducted by the complainants which would often uncover failings in the offenders scamming process.

Findings

The next section, using examples from real victims' accounts, will illustrate the anatomy of how the offenders organize the scams and the techniques they use that lead victims to fall for them. There have been only a few studies that have explored this area (see for

example Button et al., 2014; Fischer et al., 2013; Langenderfer & Shimp, 2001; Titus & Gover, 2001; Whitty, 2013, 2015) and the accounts of fraud victims (Button et al., 2014; Cross & Blackshaw, 2015; Cross et al., 2019; Prenzler, 2017). Some of the core techniques illustrated by this literature includes impersonation of official organizations, visceral appeals, time pressures, grooming victims to name some. There has also been research which has linked routine activities theory to cybercrime victimization (DeLiema, 2018; Holt & Bossler, 2008; Leukfeldt & Yar, 2016).

The quantitative findings of this investigation are illustrated in Table 1. Most of the complainants were identified as being located in the USA with a comparably smaller number located in Australia and South Africa.

The results of sorting the 415 pet deposit payment complaints into animal species and breed are presented in Table 2. The most popular animal species which the complainants were defrauded when purchasing was for pedigree puppies. The number of complainants and accumulated victim loss amounts was particularly high for Bulldog and Pomeranian puppy breeds. The victim complaints also highlighted that a smaller number of consumers were defrauded when they had attempted to purchase pedigree kittens and exotic birds.

Initial payment deposits: the 'hook'

The obtained complaints identified that a large number of victims were quick to make payment deposits on fraudulent pet websites. This is despite victims having made only limited contact with the owners of the websites and not seeing their desired pet in person or through live video-calls with the supposed breeders. Victims instead relied on gut-instinct, the legitimate appearance of fraudulent pet websites and personal emotion to guide their decision-making process. A recurring theme in the victim complaints was both the visual aesthetics of the fraudulent websites, which appeared to aid the modality's credibility, and the identification of a visually appealing photo of their desired pet which they were then keen to secure the purchase of by quickly making a payment deposit. One victim noted in their complaint that

> 'It seemed so legit, with pictures videos for the cute kitten etc' (Elizabeth).

The role of emotion not only included the visually attractive photos that the websites contained to invoke a feeling of desire but in some cases intertwined with a victim's own personal misfortunes, specifically, after a negative life event. Negative life events have been noted in previous research as a risk factor for fraud victimization (DeLiema, 2018;

Table 1. Total losses per country.

Country	Number of complainants	Loss range	Average loss per victim	Total acc. losses
Australia	4	AU$750.00–2000	AU$1287.50	AU$5150.00
USA	466	US$55.00–10,300.00	US$952.21	US$443,730.48
South Africa	11	ZAR1500–40,000	ZAR8045.45	ZAR88,500.00

Table 2. Victim complaints on pet deposit payments.

Breed	Number of victims	Total loss per breed (US$)	Average loss per victim (US$)
Puppies			
Akita	2	2599.00	1299.50
Australian Shepherd	4	2050.00	512.50
Beagle	5	2647.00	529.40
Bernedoodle	5	6950.00	1390.00
Bichon Frise	4	3400.00	850.00
Border Collie	1	1550.00	1550.00
Boston Terrier	2	3100.00	1550.00
Boxer	4	1750.00	437.50
Bulldog	72	61,877.43	859.41
Cane Corso	6	7050.00	1175.00
Cavoodle	2	2300.00	1150.00
Chihuahua	11	7470.00	679.09
Chow Chow	6	3387.00	564.50
Cockapoo	2	2250.00	1125.00
Corgi	17	18,700.00	1100.00
Dachsund	12	8197.50	683.12
Doberman	4	6135.00	1533.75
German Shepherd	2	1270.00	635.00
Golden Doodle	4	3400.00	850.00
Golden Retriever	1	550.00	550.00
Great Dane	7	6850.00	978.57
Havanese	1	500.00	500.00
Husky	6	9800.00	1633.33
Jack Russell	3	2035.00	678.33
Labradoodle	3	3660.00	1220.00
Labrador	6	5225.40	870.90
Maltese	13	11,071.50	851.65
Papillon	1	800.00	800.00
Pinscher	2	1400.00	700.00
Pitbull	14	8649.00	617.79
Pomeranian	40	35,239.41	880.99
Pomsky	4	2060.00	515.00
Poodle	18	16,150.00	897.22
Pug	17	13,310.00	782.94
Retriever	4	2132.76	533.19
Samoyed	4	2500.00	625.00
Schnauzer	8	4835.00	604.38
Shihtzu	15	9000.00	600.00
Spaniel	3	1950.00	650.00
Yorkshire Terrier	15	10,296.99	686.47
Kittens			
Bengal	7	6822.00	974.57
British Shorthair	4	2450.00	612.50

(continued)

Table 2. Continued.

Breed	Number of victims	Total loss per breed (US$)	Average loss per victim (US$)
Maine Coon	14	12,939.00	924.21
Persian	5	3050.00	610.00
Russian Blue	3	2030.00	676.67
Savannah	1	5920.00	5920.00
Siamese	1	499.00	499.00
Exotic birds			
Macaw	2	1500.00	750.00
Parrot	6	6022.50	1003.75

Ross & Smith, 2011). In the sample, the death of a close family member or a previous pet sometimes provided the rationale to contact the fraudulent seller. One victim cited the death of both her husband and previous pet as rationale for contacting the fraudulent website:

> 'My husband AND dog died last month, and I have been excited about adopting a pair of kittens because my home is pretty lonely now' (Karen).

The phenomenon of first contact being made solely by victims demonstrates a new phenomenon in cyberfraud which differs from traditional 419 fraud that instead relies on offenders spamming thousands of randomly targeted messages daily to potential victims from free email accounts (Mcguire & Dowling, 2013). This is also true in more sophisticated methods of cyberfraud that target organizations such as business–email–compromise and spear phishing that relies on imitation attacks made by offenders, spoofing an organizations CEO or vendor to obtain funds through deception (Mansfield-Devine, 2016; Wang & Winton, 2012). The development of an initial contact to groom the victim towards trust and ultimately payment has been noted by Whitty (2013, 2015) for romance scams and Olivier et al. (2015) for mass marketing frauds.

Offenders communicated with victims using an array of techniques including through email correspondences, telephone calls and text messages or WhatsApp. During this initial correspondence phase, victims often received a pre-scripted fictionalized history of the fraudulent business and were provided with promises of after-sale documentation and pet wellbeing items, in systematic attempts to enhance the legitimacy of the fraud modality. One victim's complaint provided a full transcript of an initial response to the enquiry:

> Thanks for submitting your inquiry and nice to know that you have interest in our sphinx kitten. He is still available. We are located in Allen TX, We sell each for $500 and shipping is $200. BILO will cost a total of $700 to have her shipped and home delivered. He will come along with the following papers: Health Certificate, 1 year health guarantee, Complete medical record, Crate, Playing toys, And a hand guide that will help you on basics of taking good care of the kittens. (Theodor)

The role of communicating legitimacy to victims is in stark contrast to spear phishing which relies on camouflage by spoofing legitimate organizations and a much more direct request for payment (Wang & Winton, 2012). Offenders instead chose to create their own stand-alone website and a sales process that sought to build trust and a rapport with victims before asking for payment. The process of trust building appeared to be integral in the initial scripted response sent to initial enquiries.

Religion was often emphasized in initial responses sent to victims as the underlying justification for why the prospective buyer should engage in the transaction. One victim noted how the offender attempted to pressure them, under the guise of religion to trust their website:

> 'we're a God-fearing Christian family and cheating people of their hard-earned money is not of our faith' (Mili).

Once the trust-building process had been undertaken, victims were notably pressured into making the initial deposit soon after their initial correspondences with the purported seller. The most common justification by the offender was to ensure same-day delivery. One victim's comment provided details of how the offender attempted to argue that a payment deposit was required immediately to ensure same-day delivery, despite this being impossible:

> 'Told me they can ship the pup same day and guarantee delivery to my door within 5-7 hours. Shipping from Minnesota to Ohio in 7 hours is amazing. . ..amazingly false' (Karen).

A small number of victim complaints demonstrated awareness that they were participating in a fraudulent transaction, specifically, by identifying that the pets advertised on the websites were often significantly below what they perceived to be the going-rate market price for a pet. This did not, however, detract them from pursuing the purchase. The pursuit by some of the 'too good to be true' offer provided evidence of the lack of capable guardian in some instances, supporting routine activity theory. One victim identified cost as a major factor:

> 'Because of my ambition to get the puppy soon and it was cheap, I didn't hesitate to pay' (Susan).

This was the same for a second complainant:

> 'at first they only want $600, which seems cheap but Legit' (Richard).

The offenders also sought to alleviate the concerns of victims by using excuses that it was their first litter and that this justified low prices as a method of promoting their businesses, which one victim demonstrated in their complaint:

> 'Story was it's their first litter, so the prices were low to promote themselves' (Kevin).

The complaints further identified that victims were aware that the name of the purported seller did not match with the individual that they were paying their deposit

payment to. This did not, however, appear to act as a deterrent when making a payment deposit and victims only registered this discrepancy after they had been defrauded:

> 'I should've paused when the contract name and Zelle name didn't match up' (Ivy).

In specific instances where victim complaints provided details of the money transfer, it was observed that only in a minimal amount of cases was the payment requested to be sent directly to Cameroon through historically popular domiciliary Money-gram and Western Union transfers (Tade & Aliyu, 2011). Payment was often instead requested to be sent using an additional array of non-refundable platforms including Zelle, PayPal Friends and Family and Walmart-2-Walmart transfer. In the cases of Zelle and Walmart-2-Walmart transfers, the payment deposit has to be collected within the United States demonstrating a reliance on money mules in the target country to collect victim payments and keep a commission, which is the conventionally preferred method by cybercriminals (Aston et al., 2009; Choo & Smith, 2008). The Better Business Bureau (2017) identified that in the case of pet fraud, the money mules themselves are often Cameroonian nationals operating within the United States to collect payments from victims as active facilitating parties of the fraud, often collecting sums in excess of more than half a million dollars from various money transfer collection runs and keeping a commission before sending the remaining amount back to the other members of the fraud syndicate in Cameroon.

Through the personal reasoning of the victims for making a quick purchase with little due diligence (lack of guardianship) and the rushed correspondence with the fraudulent seller, this resulted in smaller amounts from a variance of $300 to $1500 being lost in the initial deposit stage. The primary purpose of the fraud in this stage appeared to be the pressure of victims into making a single one-off smaller deposit which provided offenders with the opportunity for moving the victims onto further recurring costs which were used to defraud them of larger amounts until they eventually recognized that the pet would never arrive.

Using the non-victim complaint comments, it was also possible to identify the decision-making process which prevented some complainants from becoming victims. In the first instance, several complainants identified visible discrepancies with the fraudulent pet website which they had visited. One complainant noted how a fraudulent pet website which they had visited was being reused multiple times on the internet:

> They have changed their name to 'Betty Bull Terriers,' they have the exact same puppies up for sale and the same email address and phone number. This is their website https://betty bullterriers.com and if you compare it to https://bestbullterriers.com, you will see that it is exactly the same with very minor modifications. (Isela)

A second complainant identified that the location of a cattery did not match up with the photos on the offender's website:

> I was just looking at the website which I found to through the search engine. The one thing that got me thinking was the pictures of the kittens. (Which were oddly cheaper than normal). The cattery was supposed be in Wisconsin, but the kitten was looking out of a

> window and I saw the street below was buildings of European architecture (been over a few times so I recognize the style). Not to mention one of the cars parked there has a European license plate. (Grady)

In another case when a non-victim complainant had engaged in dialogue with an offender, the potential buyer became particularly suspicious when the offender claimed to be a local breeder from the country of purchase and instead had a particularly strong accent:

> 'I was supposed to contact the guy back tomorrow but he sounded like he was from another country heavy heavy accent and said he was American' (Pattie).

Secondary recurring fees: the 'sting'

Once victims had been defrauded in the initial deposit phase, they were in all cases re-contacted with demands for secondary larger amounts by a fake shipping company to cover the transportation and wellbeing costs derived from transporting the pet from seller to buyer. This part of the fraud modality attempted to target victims using a recovery scam, whereby victims who have previously been defrauded are revictimized through targeted techniques different to the original scam (Titus & Gover, 2001: 135). This demonstrates a new evolution of the traditional recovery scam by instead targeting victims immediately after they had been immediately defrauded and utilizing the same modality, albeit a different part of the purchase phase, to revictimize previous victims (Titus & Gover, 2001: 135).

The victim complaints identified that offenders created a second website, a shipping company, and provided victims with a tracking code so that they could track the shipping process of the pet on the website, subject to the payment of fees. The most popular fee presented to victims was an urgent request to change the shipping crate from an 'original' to a 'temperature controlled' shipping crate to ensure that the body temperature of the pet would remain constant during the shipping process and to resist the 'harsh temperature of the atmospheric conditions'. Victims were also presented with a range of crates which required deposit that the offender claimed would be fully refunded upon receipt of the pet if the buyer did not want to own the crate. Other fictitious costs introduced at this stage also included veterinary and quarantine fees, registration documentation fees and insurance fees. Most victims during this stage refused to pay the additional amounts, often conducting their own research to disprove that these fees would be part of a legitimate shipping process. One victim did not pay for the temperature-controlled crate after conducting her own research:

> 'planes already have pressure and climate control in their cargo areas' (Julie).

Another victim identified discrepancies with the shipping website, stating that

> 'The anti-pressure crate picture shows a regular pet crate with the open metal grid front door' (Todd).

The few victims that paid these secondary recurring fees were defrauded relative to the amount of payments that they had made. The lowest figure that a victim was defrauded of was for a $99 one-off shipping fee, despite earlier paying a deposit amount of $400 for a kitten. The highest figure was for $10,000 which involved a situation whereby the offender claimed that there had been a plane crash and the puppy died. This situation, the offender claimed, had resulted in the breeder suing the shipping company. In this case, the victim paid for the fictitious and unspecified court costs.

During the shipping stage of the modality, many victims threatened the withdrawal of their cooperation by not paying the secondary fees. The offender would then attempt to prevent the loss of cooperation and pull the victim back on track through techniques of extortion by threatening the buyer with fines. The most popular threat used was that if the victim refused to pay for the additional shipping fee then the buyer would receive a 'puppy abandonment' fine. Furthermore, in some cases the fraudulent seller would threaten the buyer with action from law enforcement: that the police would enter their property and remove all of their current pets before registering the buyer as an animal abuser. The US Drug Enforcement Agency has identified similar tactics used against victims of fraud who had attempted to purchase drugs over the internet where they had later been threatened with 'fines' to avoid law enforcement action being taken against them (Drug Enforcement Agency, 2019). In the case of pet fraud, the modality remains somewhat more ambiguous with offenders stating that fines would be produced from 'court' or the 'police' in the case of 'puppy abandonment'.

Opportunity for adaptability: COVID-19

Scammers are often innovative, exploiting new opportunities that arise to maximize returns from victims (Button et al., 2009; Fischer et al., 2009). As Braucher & Orbach (2015) have argued, 'Successful scammers-individual or institutional ones-are opportunistic and take advantage of circumstances.' Crises and disasters bring new opportunities to be exploited by offenders with potential victims in a desperate state more susceptible to falling for them (Frailing & Harper, 2017; Kerstein, 2006). COVID-19 has yielded dozens of new opportunities for scammers. The demand for pets among people stuck in their homes self-isolating persons has led to new innovations in pet scams. Victim comments identified that COVID-19 was being actively incorporated into the shipping fee stage of the defrauding process as potential buyers have been forced to stay isolated and purchase pets over the internet without being accustomed to spotting the warning signs of a fake website (Fraud.org, 2020). One victim from Australia complained that they had been requested to purchase a 'special shipping crate' to ensure that their purchased puppy could fly during the lockdown despite air travel being highly restricted:

> I cannot believe I didn't see the warning signs sooner until I got to the delivery stage and they asked for over $1000 for a special crate for Covid-19 safe travel on the plane out of Burnie, Tasmania, which was locked down last week! (Samantha)

A second complainants comments identified that COVID-19 was being utilized as an opportunity for the offender to circumnavigate the process of utilizing money mules for

the collection of stolen funds by instead seeking direct remittance of the stolen funds to Cameroon resulting from a lack of opportunity for money mules to make domestic payments: 'I sent the money but after he told me that the banks don't work and I should send the money to his office in Cameroon, because of covid-19 the banks in US don't work' (Nikolay).

Conclusion and discussion

The huge increases in frauds facilitated by the opportunities from the changes in shopping, that the internet has enabled, have to date only sparked limited interest from criminologists compared to traditional volume crimes (Button & Cross, 2017; Levi, 2016; McGuire, 2018). The colossal array of frauds and scams that have emerged provide for a substantial criminal landscape to research. Pet scams are just one type of this vast range of new crimes and this article has provided a unique insight on this form of advance fee and non-delivery fraud common in the USA, Australia and South Africa. Several academics have noted the importance of routine activities in explaining greater online victimization of cybercrime (DeLiema, 2018; Holt & Bossler, 2008; Leukfeldt & Yar, 2016). The significant changes in the nature of shopping, which has also developed with the purchase of pets has caused a variety of new criminal opportunities. The routine of online shopping, including for pets, augmented by the COVID-19 crisis has contributed to increased risk of victimization. As our means of shopping has changed so has the criminal risks we face. Motivated offenders can target a large number of victims through their 'honeypot' sites, many of whom lack the foundations of a capable guardian – thus providing all the ingredients for victimization to occur.

The deconstruction of pet scams using victim accounts undertaken in this paper has revealed the common techniques used, which are prevalent in many other types of scams. This research highlighted the techniques of impersonation, with authentic looking websites that provoke visceral responses with images of the most appealing pets; time pressures that force victims into hasty decisions, providing a hook that once in, lures them into a sequence of further payments they must make to avoid 'losing' the initial stake; with payments arranged through preferred anonymous and less safe methods. The deconstruction of these scams, however, also provides the clues to better preventing them, using such knowledge helps law enforcement and appropriate voluntary groups to pursue preventative strategies and ultimately educate and equip potential victims to reduce their risk to such crimes. Online shopping will continue to grow and with that increased risks of fraud, understanding the techniques of fraudsters in different online shopping modalities is central to better preventing it.

Such frauds also raise a number of issues that have been only touched upon in this article. Perhaps one of the most salient is the important role played by victim oriented voluntary organizations. Petscams.com with its unique set of data and knowledge on a niche advance fee fraud scam has a potent capability for supporting pet buyers to avoid victimization and support law enforcement in combatting it by providing victims and other external stakeholders with the opportunity to interact in a unique way through a moderated multi stakeholder platform. Such 'responsibilization' (Garland, 1996) of crime prevention at the international and cyber level clearly has benefits for all, but such digilanteism – at least in the form of those such as 419Eater – has received largely

critical attention (Button, 2019; Byrne, 2013). Clearly, a more nuanced assessment of the potential for such entities needs to be developed.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD


Jack M Whittaker https://orcid.org/0000-0002-3669-9066

References

Abia, W. A., Jato, D. M., Agejo, P. A., Abia, E. A., Njuacha, G. E., Amana, D. A., Akebe, L. K., Takang, A. S. J., & Ekuri, D. O. (2010). Cameroonian youths, their attractions to scamming and strategies to divert attention. *International NGO Journal*, *5*(5), 110–116.

Ablon, L., & Libicki, M. (2015). Hackers' Bazaar: The markets for cybercrime tools and stolen data. *Defense Counsel Journal*, *82*(2), 143–152. https://doi.org/10.12690/0161-8202-82.2.143

Alba, J., Lynch, J., Weitz, B., Janiszewski, C., Lutz, R., Sawyer, A., & Wood, S. (1997). Interactive home shopping: Consumer, retailer, and manufacturer incentives to participate in electronic marketplaces. *Journal of Marketing*, *61*(3), 38. https://doi.org/10.2307/1251788

Almendra, V. (2013). Finding the needle: A risk-based ranking of product listings at online auction sites for non-delivery fraud prediction. *Expert Systems with Applications*, *40*(12), 4805–4811. https://doi.org/10.1016/j.eswa.2013.02.027

Ampratwum, E. (2009). Advance fee fraud "419" and investor confidence in the economies of sub-Saharan African (SSA). *Journal of Financial Crime*, *16*(1), 67–79. https://doi.org/10.1108/13590790910924975

Aston, M., McCombie, M., Reardon, S., & Watters, P. (2009). A preliminary profiling of internet money mules: An Australian perspective. In *Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing* (pp. 482–487). IEEE Computer Society.

Better Business Bureau. (2017). *Puppy scams: How fake online pet sellers steal from unsuspecting pet buyers*. https://www.bbb.org/globalassets/article-library/puppy-scam-study/puppy-scams-bbb-study-20170901.pdf

Boddy, M. (2018). Phishing 2.0: The new evolution in cybercrime. *Computer Fraud & Security*, *2018*(11), 8–10. https://doi.org/10.1016/s1361-3723(18)30108-8

Braucher, J., & Orbach, B. (2015). Scamming: The misunderstood confidence man. *Yale Journal of Law & the Humanities*, *27*(2), 249–290.

Button, M. (2019). *Private policing* (2nd ed.). Routledge.

Button, M. (2020). The "new" private security industry, the private policing of cyberspace and the regulatory questions. *Journal of Contemporary Criminal Justice*, *36*(1), 39–55. https://doi.org/10.1080/01639625.2020.1717840

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims* (1st ed.). Routledge.

Button, M., Lewis, C., & Tapley, J. (2009). *A better deal for fraud victims: Research into victims' needs and experiences*. National Fraud Authority.

Button, M., Nicholls, C., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Byrne, D. N. (2013). 419 digilantes and the frontier of radical justice online. *Radical History Review*, *2013*(117), 70–82.

Chaudhry, P., & Stumpf, S. (2011). Consumer complicity with counterfeit products. *Journal of Consumer Marketing*, *28*(2), 139–151. https://doi.org/10.1108/07363761111115980

Choo, K., & Smith, R. (2008). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology*, *3*(1), 37–59. https://doi.org/10.1007/s11417-007-9035-y

Chouhan, R. (2014). Cyber crimes: Evolution, detection and future challenges. *The IUP Journal of Information Technology*, *X*(1), 48–55.

Corbin, J., & Strauss, A. (1990). *Basics of qualitative research: Techniques & procedures for developing grounded theory* (4th ed.). Sage Publications.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187–204. https://doi.org/10.1177/0269758015571471

Cross, C., & Blackshaw, D. (2015). Improving the police response to online fraud. *Policing*, *9*(2), 119–128. https://doi.org/10.1093/police/pau044

Cross, C., Parker, M., & Sansom, D. (2019). Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. *International Review of Victimology*, *25*(1), 53–69. https://doi.org/10.1177/0269758017752410

DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist*, *58*(4), 706–718. https://doi.org/10.1093/geront/gnw258

Dion, M. (2010). Advance fee fraud letters as Machiavellian/Narcissistic narratives. *International Journal of Cyber Criminology*, *4*(1), 630–642.

Drug Enforcement Agency. (2019). *Alert – Extortion scam targeting DEA registrants*. Dea.gov. Retrieved, July 11, 2020, from https://www.dea.gov/stories/2019/06/11/alert-extortion-scam-targeting-dea-registrants

Durkin, K., & Brinkman, R. (2009). 419 fraud: A crime without borders in a postmodern world. *International Review of Modern Sociology*, *35*(2), 271–283.

Fischer, P., Lea, S., & Evans, K. (2009). *The psychology of scams: Provoking and committing errors of judgement*. *Research for the Office of Fair Trading*. University of Exeter.

Fischer, P., Lea, S., & Evans, K. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology*, *43*(10), 2060–2072. https://doi.org/10.1111/jasp.12158

Frailing, K., & Harper, D. (2017). *Toward a criminology of disaster* (1st ed., pp. 109–139). Palgrave Macmillan.

Fraud.org. (2020). *Fueled by COVID-19, pet adoption scams on the rise*. Fraud.org. Retrieved, June 22, 2020, from https://www.fraud.org/coronavirus_pet_scams

Garland, D. (1996). The limits of the sovereign state strategies of crime control in contemporary society. *The British Journal of Criminology*, *36*(4), 445–471.

Holt, T., & Graves, D. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology*, *1*(1), 137–154. https://doi.org/10.5281/zenodo.18282

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Kerstein, F. A. (2006). An overview of post-disaster fraud. *St Thomas Law Review*, *18*(3), 791–802.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, *80*(3), 541–555. https://doi.org/10.1016/j.techfore.2012.07.002

Langenderfer, J., & Shimp, T. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology and Marketing*, *18*(7), 763–783. https://doi.org/10.1002/mar.1029

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Levi, M. (2016). *The implications of economic cybercrime for policing* (p. 8). City of London Corporation.

Lynch, J., & Ariely, D. (2000). Wine online: Search costs affect competition on price, quality, and distribution. *Marketing Science*, *19*(1), 83–103. https://doi.org/10.1287/mksc.19.1.83.15183

Magnusson, D. (2009). The costs of implementing the anti-money laundering regulations in Sweden. *Journal of Money Laundering Control*, *12*(2), 101–112. https://doi.org/10.1108/13685200910951884

Manky, D. (2013). Cybercrime as a service: A very modern business. *Computer Fraud & Security*, *2013*(6), 9–13. https://doi.org/10.1016/s1361-3723(13)70053-8

Mansfield-Devine, S. (2016). Ransomware: Taking businesses hostage. *Network Security*, *2016*(10), 8–17. https://doi.org/10.1016/s1353-4858(16)30096-4

Mcguire, M. (2018). *Into the web of profit: Understanding the growth of the cybercrime economy* (p. 15). Bromium Inc.

Mcguire, M., & Dowling, S. (2013). *Cybercrime a review of the evidence (Research Report 75). Chapter 4: Improving the cybercrime evidence base*. Home Office. Retrieved, April 28, 2020, from http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246756/horr75-chap4.pdf

Olivier, S., Burls, T., Fenge, L. A., & Brown, K. (2015). "Winning and losing": Vulnerability to mass marketing fraud. *The Journal of Adult Protection*, *17*(6), 360–370. https://doi.org/10.1108/JAP-02-2015-0002

Prenzler, T. (2017). Fraud victimisation and prevention. In *The Palgrave handbook of Australian and New Zealand criminology, crime and justice* (pp. 269–283). Palgrave Macmillan.

Rohm, A., & Swaminathan, V. (2004). A typology of online shoppers based on shopping motivations. *Journal of Business Research*, *57*(7), 748–757. https://doi.org/10.1016/s0148-2963(02)00351-x

Ross, S., & Smith, R. G. (2011). *Risk factors for advance fee fraud victimisation*. Australian Institute of Criminology, Trends and Issues in Crime and Criminal Justice No. 420. https://core.ac.uk/download/pdf/30680737.pdf

Shaw, M. (1994). Civil society and global politics: Beyond a social movements approach. *Millennium: Journal of International Studies*, *23*(3), 647–667. https://doi.org/10.1177/03058298940230031001

Sheth, J. (1983). Cross-cultural influences on the buyer-seller interaction/negotiation process. *Asia Pacific Journal of Management*, *1*(1), 46–55. https://doi.org/10.1007/bf01734310

Soomro, T., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems*, *24*(1), 9–17. https://doi.org/10.2478/acss-2019-0002

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal*, *32*(3), 342–361. https://doi.org/10.1057/s41284-019-00166-w

Strauss, A. (1987). *Qualitative analysis for social scientists* (1st ed.). Cambridge University Press.

Swaminathan, V., & Lepowska-White, E. (1999). Browsers or buyers in cyberspace? An investigation of factors influencing electronic exchange. *Journal of Computer-Mediated Communication*, *5*(2). https://doi.org/10.1111/j.1083-6101.1999.tb00335.x

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860–875.

Titus, R. M., & Gover, A. R. (2001). Personal fraud: The victims and the scams. In Repeat victimization, *crime prevention studies* (12th ed., pp. 133–152). Criminal Justice Press.

Van Wilsem, J. (2011). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178. https://doi.org/10.1093/esr/jcr053

Wang, T., & Winton, A. (2012). Competition and corporate fraud waves. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2103386

Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF): Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science & Management*, *19*(1), 39–53. https://doi.org/10.1177/1461355716681810

Whitty, M. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665–684. https://doi.org/10.1093/bjc/azt009

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443–455. https://doi.org/10.1057/sj.2012.57

Young, J. (2019). *Global ecommerce sales to reach nearly $3.46 trillion in 2019*. Digital Commerce 360. Retrieved, May 4, 2020, from https://www.digitalcommerce360.com/article/global-ecommerce-sales/