The Check is in the Mail: Monetization of Craigslist Buyer Scams

Jackie Jones
Information Technology
George Mason University
jjones24@masonlive.gmu.edu

Damon McCoy
Computer Science
George Mason University
mccoy@cs.gmu.edu

***Abstract*—Nigerian or advance fee fraud scams continue to gain prevelance within the world of online classified advertisements. As law enforcement, user training, and website technologies improve to thwart known techniques, scammers continue to evolve their methods of targeting victims and monetizing their scam methods. As our understanding of the underground scammer community and their methods grows, we gain a greater insight about the critical points of disruption to interrupt the scammers ability to succeed. In this paper we extend on previous works about fake payment scams targeting Craigslist. To grow our understanding of scammer methods and how they monetize these scams, we utilize a data collection system posting "honeypot advertisements" on Craigslist offering products for sale and interact with scammers gathering information on their payment methods. We then conduct an analysis of 75 days worth of data to better understand the scammer's patterns, supporting agents, geolocations, and methods used to perpetuate fraudulent payments. Our analysis shows that 5 groups are responsible for over 50% of the scam payments received. These groups operate primarily out of Nigeria, but use the services of agents within the United States to facilitate the sending and receiving of payments and shipping of products to addresses both in Nigeria and the United States. This small number of scammer organizations combined with the necessity of support agents within the United States indicate areas for potential targeting and disruption of the key scammer groups.**

I. Introduction

Advance fee fraud scams, also known as Nigerian "419" scams, have been around for centuries, changing and expanding as technology and world events change [1]. With the advent of the Internet, these scams moved online, at first in spam and emails, and more recently in online classified advertisements and dating sites. Targeting both businesses and individuals, these scams result in financial losses of billions of dollars a year [2], but also a psychological impact against their victims [3]. Today, the sophistication of online scams continues to grow and improve as new technologies allow scammers more venues for access to victims and improved capabilities for monetization of their scams.

Craigslist and other online sites have established many safeguards to filter out scam postings and protect users from fraud, such a phone verification, blacklisting IP addresses and monitoring for suspicious content. However, the majority of these safeguards are focused on preventing scammers from posting fraudulent information on the site, little effort has been made to protect legitimate users receiving responses from fraudulent buyers. In 2013, a research measurement study was conducted focusing on the fake payment scams targeting users on Craigslist [4]. One result of the study was the identification of two primary payment methods, fake checks and fake Paypal payments being utilized by scammer groups in furtherance of their scam attempts.

This paper focuses on these two payment methods in order to gain insight into the scammer organizations and economy, their structure, methods and objectives with the aim to better understand this niche of the Nigerian scam economy and seek intervention points. The questions addressed include: "How do these organizations monetize their scams?", "What support infrastructure is necessary for these fake payments to be processed?", "What additional features can we identify to distinguish scam attempts from legitimate Craigslist postings?".

Identification of Nigerian scammers posing as buyers on Craigslist has been found to be susceptible to honeypot advertisements. Therefore, we use a similar methodology to identify and target the scammers. We chose a manual data collection system for all Craigslist postings, collection of emails and interaction with scammers in order to personalize responses, extend out conversations beyond scammer automated responses and force scammers to interact at a personal level in hopes this would reveal additional information. We collected IP addresses of scammers and performed analysis of the collected dataset to cluster the scammers into organizational groups based on key factors such as email addresses, shipping addresses and phone numbers but also with additional factors identified during the fake payments portion of the scam including business addresses and signatures on fake checks, "mover" agent addresses and mail return addresses.

Our analysis corroborated similar results to previous studies [4] regarding a small number of organizations being responsible for over 50% of the fake payments and groups using multiple initial email accounts filtering down to a smaller number of reply-to email accounts. Of interest though was the analysis result that the majority of fake Paypal payments scams resulted in direct shipment requests to Nigeria while all fake check payment scams led to addresses within the United States.

Our analysis shows that the choice of the payment method is related to the monetization method sought by the scammer,

either scamming the victim out of the product being sold on Craigslist (fake Paypal), scamming money directly from the seller (fake Paypal with a mover agent) or scamming money from a third party victim (fake check with a mover agent), although small overlap does occur. This analysis indicates that several factors such as law enforcement techniques, user education and availability of scammer support personnel within the United States can all impact the online scam community and the scammers ability to monetize the actions. Additionally, the identification of stateside addresses used in furtherance of these scams and the limited number of organizations accounting for the majority of the scam attempts further indicates the possibility to identify, target and disrupt the key groups having the most impact on the scam landscape.

II. Related Works

Previous studies have focused on understanding the basics of Nigerian scams targeting Craigslist and how the scammer groups are organized [4]. Some studies have looked at the cultural issues faced by the youth in Nigeria that have given rise to the scammer culture prevalent there [5], [6]. Additionally, several studies have focused on the Nigerian 419 scams and related advance fee fraud methods across other platforms [7] and other scam methods targeting both social media and online auction sites [3], [8]. Herley's research [9] relates how scammers craft their messages to focus their efforts and filter out victims unlikely to fall for their scam attempts corresponds to the crafting of our advertisements to identify potential scammers and filter out legitimate Craigslist users. While previous research focused solely on the collection of online empirical data gathered through automated email interactions with scammers, this research added additional elements of data collected through manual online and offline interactions, primarily through analysis of the fake checks mailed by the scammers and their methods of transportation.

Another collection of works has focused on the role of the money mule in the extraction and anonymous exfiltration of money from the victim to the scammer [10], [11]. Moore's work [12] explains how *"the mule becomes personally liable for the funds already sent."* These works primarily focus on the role of mules within the phishing scams, while we explore the similar role of money mules within the online advertiser scam community, including the role the victim plays within the money mule chain.

III. Data Collection Methodology

We used a technique similar to a previous methodology in attracting scammers to our Craigslist postings [4]. However, instead of an automated collection methodology, we chose to use manual data collection in order to enhance our ability to personalize and extend our online interactions with targeted scammers. Our hope was to increase our success rate in moving negotiations beyond initial emails and automated responses by the scammers and thereby map out the deeper layers of the scams not accessible through purely technical means. Figure 1 illustrates our data collection methodology, including the various payment methods used by the scammers and outlined in Section IV-A.

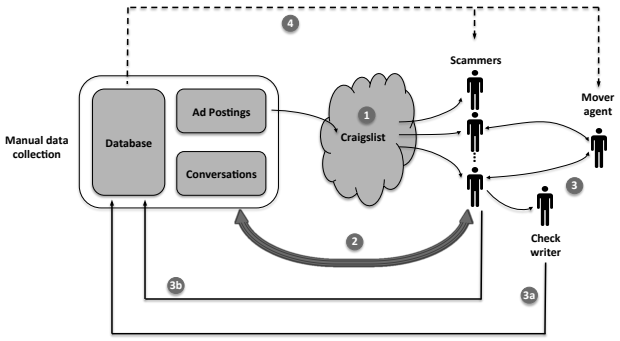

Fig. 1: **Scam data collection.**
(**1**): Post "unattractive" honeypot ads to attract only scammers;
(**2**): scammers respond to ads and enter negotiations;
(**3**): scammers may use others to facilitate payments;
(**3a**): fraudulent checks are mailed as payments;
(**3b**): or fraudulent paypal payments are made;
(**4**): scammers anticipate money and products will be shipped (not during this experiment);

A. Creation of honeypot posts

We created "honeypot" advertisements designed to selectively attract scammers while purposely being unattractive to legitimate users as implemented during our previous research. We posted unattractive advertisements selling used laptop computers at prices slightly higher than they were worth as advertised on Amazon.com. Legitimate users would not be attracted to the used products that could be found cheaper on Amazon, however scammers using automated crawlers targeting Craigslist would respond to such advertisements. We conformed to good ethical standards in our data collection methods as discussed in Section III-D below.

B. Communication with scammers

Utilizing multiple email accounts generated through Google Mail (Gmail) and subsequent Craigslist accounts tied to those Gmail accounts we entered into negotiations with all responses to our advertisements, personalizing the responses to move beyond the scammer automated responses as quickly as possible. By purposely failing to provide all the information requested by scammers and asking our own follow-on questions, we sought to force scammers to personally respond during the negotiation process.

C. IP address collection

As identified in previous research and confirmed during this project, the majority of scammers utilize Gmail accounts. Since this webmail provider does not include the source IP address in its email headers and utilizes proxy servers to serve embedded images rather than displaying the image from our original host server, we included image links within our emails in order to entice scammers to click on the link to our web

server hosting the image and thereby allowing us to capture the IP address for further analysis. We assumed that scammer automated responses would not access the embedded links, this was one of the driving factors for extending the conversations beyond the automated response stages and engaging the scammer directly before providing the image links, increasing the likelihood of our capturing the IP address of the scammer.

D. Ethics

Our research study deals with interactions with human subjects and therefore controls were set in place to manage any potential harm to associated stakeholders. Our institution human subject's review board also approved our research. Honeypot advertisements were designed to be unattractive to legitimate Craigslist users, however in the event of actual payment attempts by a legitimate user we purposely failed to set up a corresponding Paypal account based on our Gmail accounts thereby ensuring we would never receive any actual funds via this payment method. Additionally, no attempt was made to cash any of the checks received although we did go to banks in an effort to discover more information and ways to identify the checks as fraudulent. In the event an actual payment was made then the actual product being advertised was on hand to be shipped to the legitimate Craigslist buyer in order to fulfill our contractual responsibilities in accordance with the accepted user agreement with Craigslist. During the course of this research we only identified one respondent as being a legitimate Craigslist user and ceased negotiations with that potential buyer immediately upon identification before negotiations moved to the payment stage.

While during the course of this research we did collect many elements of personal information such as addresses and phone numbers, which could be used to identify individuals, this information will not be included in our results and only aggregate information will be included.

Finally we adhered to Craigslist's terms of use regarding the posting of advertisements[1], intentionally limiting ourselves to one advertisement per account at a time.

IV. Experimental Results

In Sections IV and V we present a summary of our collected dataset then our findings from this measurement study.

A. Overview of scam monetization methods

During this study we identified three primary methods of monetization associated with this form of Craigslist scams, theft of the seller's product, theft of the seller's money and theft of a third party's money. The latter form of monetization was the most interesting as it required support from multiple individuals besides the scammer in order to achieve success and therefore gave the greatest insight into the organization and conduct of scammer operations.

[1]http://www.craigslist.org/about/terms.of.use

1) Product as the objective: This form of scam is the simplest of the monetization methods identified and correlates to theft of the product due to failure to submit remuneration. The buyer offers to purchase the product being sold online, but for various reasons (out of town, present for a relative, in the hospital, etc.) cannot pick up the product themselves and needs us, as the seller, to ship the product, usually not to the buyer directly, but to the friend or relative for whom they are buying the product. Payment is made via Paypal and subsequently we receive several emails, ostensibly from Paypal, saying the payment from the buyer has been received but is being held in escrow by Paypal until proof of product shipment is supplied. The emails stipulate that once we ship the product and provide the shipping tracking number, the money will be credited to our Paypal account. However, once the product has shipped, then of course no payment is made, and either all communication with the buyer ends, or else a series of delays/excuses are made as to why the payment is not be credited to the seller, delaying the seller from taking any action until the scammer receives the product.

This form of scam requires no overt additional support beyond the scammer as they can generate all the emails, including the fake Paypal emails, from anywhere and have the product shipped directly to them.

2) Seller's money as the objective: This form of monetization uses a version of the advance fee fraud. The buyer offers to purchase the product using Paypal as the payment method, with a third-party, a "mover" agent, coming to pick up the product. However, due to a variety of reasons (out of country, onboard a ship, recent identity theft, etc.) the buyer is unable to pay the mover directly and needs assistance from us as the seller. Additional money, averaging $486, is included above the payment for the item. As with the previous monetization method, emails are generated by a fake Paypal site that the money has been transferred and is being held in escrow until verification of payment to the mover agent has been made by a one-way money transfer method such as Western Union or Moneygram. Since no money has been released by Paypal, the seller must pay the mover agent with their own money with the hope of being reimbursed once the funds are released from escrow. Once payment to the mover agent has been made, either all communications cease, or the buyer states that the product must also be mailed before Paypal can release the funds, resulting the both lost money and lost product for the seller.

The most common money transfer mechanism was via Western Union to a mover agent at an address within the United States. Funds transferred via Western Union must be picked up in the city and state to which the money is sent and therefore this requires an individual located within the United States to act as the mover agent and receive the transferred funds. While this could potentially be the scammer, based on IP address analysis, the majority of the scammers operate from overseas (usually Nigeria) and therefore are not the ones directly receiving the money via the wire transfer. It is assumed

that the mover agent is acting as a money mule[2] and after keeping a share of the proceeds, they transfer the majority of the funds on to the scammer.

Since this version requires the seller to pay additional money out-of-pocket, the amount asked for by the scammer must be high enough to make the scam worthwhile, including the portion going to the mover agent, while also low enough not to scare off the buyer from completing the payment. This is the basis for the low amount of additional money ($486) asked by the scammer to be sent to the mover agent compared to other versions of this scam.

3) Third party's money as the objective: A similar advance fee fraud, in this monetization method the buyer offers to pay via a certified check, but again, they cannot pick up the product themselves and wish to use a mover agent. Claiming to have multiple items being picked up in the area, and since they cannot pay the agent directly, they need the seller's help to pay the mover agent. Therefore the payment will include a much larger amount, averaging ˜$1,500, above the price of the item being purchased. Upon receipt, the seller needs to cash the check, keep their portion of the money, and then send the "mover" agent their share of the payment, again via an irreversible payment method such as Western Union. Once the "mover" is paid then again all communications cease or else shipment of the product is requested.

This form of the scam again requires the support of additional individuals within the United States. Analysis of the IP addresses accessing the embedded photos shows that the majority of the scammers reside overseas (Nigeria), however one individual must print off the fake check and mail it to the buyer while another individual acts as the "mover" agent to receive the funds, both located within the United States[3]. Analysis of the various addresses associated with these checks, detailed in section IV-D below, shows that in some cases the check writer and the mover agent may be the same person while in others they are clearly separate individuals.

This method differs from the method above in that the check is seemingly legitimate enough that is will be cashed by the bank and the seller will receive the funds for their item and the funds to pay the "mover". However, when it is discovered that the check is fake, from either a stolen or non-existent account, the bank will contact the seller for possible recoupment of lost funds as they cashed the check. Since the fraudulent checks are designed to be cashed by the seller, the money being sent to the mover agent does not initially come out of the seller's pocket, in fact, the seller receives payment for their sale which is not the case in either previous methods. Final recoupment of lost funds depends on the seller's relationship with their bank where the check was cashed. Bank policy will dictate whether an account can float the full or partial amount of funds during the check verification (clearing) process. This policy depends on the bank and can result in the bank losing money if the seller does not have enough money in the account to repay the bank once the check fails to clear. The bank may then seek to find the mover agent, recoup only a portion of the money from the seller, hold the seller liable for the entire amount or write off the money as a loss. Since the seller receives payment for the item and forwards money to the mover agent that is not from their own pocket distinguishes this variation of the scam from the previous version with payment via Paypal where the seller never receives payment and pays the mover agent from their own money.

The fact that the seller receives their payment is the basis for the higher amount of money ($1,500) the scammer asks be sent to the mover agent. A higher profit margin is therefore available for the scammer even with the addition of a second individual, the check writer, receiving a portion of the money. However, this method also incurs additional costs for the scammer organization. The necessary authenticity of the checks requires the purchase of check writing software and special paper, and mailing the checks also requires the expenditure of money prior to payout from the scam.

B. Dataset

Overview: Our dataset (Table I) was gathered over a 75-day period from 2/22/2014 to 5/7/2014. Products advertised were laptop computers of various models with prices ranging from $250-$1,350. 86 payments were made totaling nearly $140,000. The average check payment was for $1,953.58 and the average paypal payment was $1,065.64. The total amount of money, that could be identified, the scammers asked to be forwarded to "mover" agents was $61,945.14 and averaged $1,346.63 per transaction (46 transactions). Several factors impact the profit margin of the scammer organizations including the number of people targeted and the conversion/success rate of the scam, payments to individuals supporting the scam such as check mailers and money mules and the operating costs of producing and mailing fake checks. Since we were unable to verify or estimate these costs we are unable to provide an estimate of the profitability of this scam.

A total of 1,315 emails were received and 824 emails were sent during this period. Emails within the same conversation are referred to as a thread, and emails were categorized based on commonalities such as email address, phone number, the various addresses associated with each monetization method and attributes of the checks, in order to group and associate threads to individual scammers/groups.

C. Analysis of checks

As stated in section IV-A-3 above, when the monetization method included payment via check, this allowed for the greatest insight into the scammer operation based on two factors. First, this method was the only time an actual physical item was transferred from the buyer (scammer) to the seller, and second, this method requires support from individuals within the United States. Figure 2 shows two checks received during this study. Note that though the checks are from

[2]It is unclear if the money mules are willing participants in this scam or the victims of a scam that are unwittingly acting as money mules.

[3]Again, it is unclear if these mover agents are willing or unwittingly participants in this scam

Overview	Duration of experiment	75 days (2/22/2014 - 5/7/2014)
Honeypot Ads	Total number of ads	56
Emails	Emails received	1,315
	Emails sent	824
	Email threads	309
Payments	Total check amounts	54 ($105,493.14)
	Total paypal amounts	32 ($34,100.53)
	Sum of all payments	$139,593.67
	”Mover” agent payments	46 ($61,945.14)
Shipping Addresses	Money mules	43
	Product shipments	21

TABLE I: **Summary of results.**

Fig. 2: **Samples of received checks.**

different companies on opposite sides of the US, the signatures are the same.

1) Check characteristics: Of all the checks received, only one was written by hand, all other checks were printed using check writing software, such as VersaCheck, using legitimate check paper, based on the existance of watermarks and other security features. Several of the checks arrived as part of a complete 8 1/2” X 11” sheet of check writing paper perforated into thirds for the printing of multiple checks, although only one check was printed at a time.

We looked up all the bank routing numbers on the checks and found that all were correctly associated with the bank and addresses written on each check, and that, where identifiable, 73% (24 of 33) of the banks were located within or near the city of the business address on each check. No personal checks were received, only business addresses, and over 90% (30 of 33) were found to be legitimate businesses based on internet searches. There was no pattern found for either large or small businesses being used as part of these scams. Some were small-scale businesses such as auto parts stores and gas stations, while others were universities, churches, and city government offices.

Several checks were taken to the bank listed on the check (although to a different branch office) and asked about the legitimacy of the checks as received. Each bank stated that from their observations, the checks looked legitimate and would probably be cashed. However, there are two elements on each check that cannot be verified by the cashing bank, the account number and the signature. Those features would be verified by the bank of origin and presumably at that point it would be discovered that the check was fraudulent. Bank privacy rules prevented our verification of both the account number and signatures being associated with the business located on the checks.

We did identify that many of the fraudulent checks bore the same signatures, even from businesses widely dispersed across the country. One signature was used on six different checks from three different states. These signatures were used to associate and further classify scammer organizations.

Service	%	Average Cost
USPS (2-day)	69% (37)	$5.60
UPS (next day)	22% (12)	$61.21
FEDEX (2-day)	9% (5)	$23.10

TABLE II: **Mail services utilized for check delivery.**

D. Analysis of Addresses

Since the use of fake checks is the only method where there is physical receipt of payment between the scammer and the seller, this method provided for the increased data gathered during this research.

The scammers attempt to rapidly monetize their scams, so all the checks received were sent via either overnight or two-day mail service using the United States Postal System (USPS), United Parcel Service (UPS) or Federal Express (FEDEX). The mail service and percentages associated with each are shown in Table II, along with the average costs associated with each mailing. This cost was calculated by recreating the mailing on the associated mail service website from the city/state the letter originated from to the shipping addresses we used to receive mail from the scammers and finding the associated cost for the appropriate delivery method. Since each of these mail services include tracking numbers for their expedited mail, the scammers themselves tracked the delivery notifications and would rapidly resume email contact pushing for us to send the money to the mover agent. Table III

Address Type	Verifiable?
City/State of mail origin	Yes
Return address on envelope	No
Business address on check	No
Bank address on check	No
Mover agent address	Yes *

TABLE III: **Addresses associated with fraudulent checks.**
* City/State is verifiable, although street address is unreliable.

outlines the five different addresses available from each fraudulent check and the likelihood each type of address is verifiable as providing information about the scammer organization. For example, although the bank addresses are legitimate branch offices, it is unlikely that the fraudulent checks are for either actual accounts at that bank or that those accounts belonged to anyone in the scammer organization. Several attempts to verify account numbers at the banks through the use of small deposits were rejected.

We found that the scammers use different addresses across multiple states in a presumed effort to cause confusion when the victim seeks to recoup lost monies. The more names and businesses associated with each check increases the difficulty with determining responsibility.

While we were not able to verify if any of these businesses were complicit in the scam, significant effort was put forth in the creation of these fraudulent checks to make them seem as genuine as possible. This assessment is based on the legitimate nature of the businesses, the bank address and routing number being from the same city as the businesses, the costly check writing software and check paper being used in the check creation. This level of detail is necessary for this type of scam since the check must pass inspection by the bank and be cashed in order for the victim to be able to access the money and send it to the mover agent.

By comparing these addresses to other addresses identified in this and from our previous research study we were able to improve our classification of scammer organizations strategy and increase our ability to identify the large scammer groups operating as buyers on Craigslist. In addition, the signature on each check was also compared for inclusion into the categorization of email threads and classification of scammer groups. A breakdown of each address group by state follows showing the top 5 states from each category.

1) City/State checks mailed from: Since all checks are mailed with tracking numbers, we were able to identify the city and state where the check was actually mailed. Figure 3 shows that Texas (16 checks, 9 different cities) and California (10 checks, 6 different cities) are the origin for almost half of the fake checks received, with some cities being the origin for multiple checks. Since our IP analysis shows that the majority of check scammers operate from Nigeria, then the origin of the checks indicates that the scammers are utilizing the services of an accomplice within the US to print and mail the checks.

Since this information only provides the city and state the check was mailed from, we did not include this feature

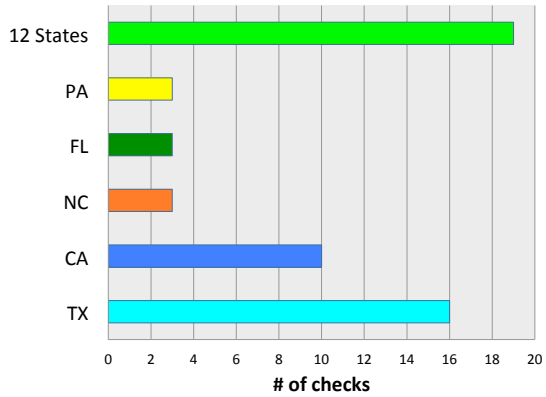

Fig. 3: **Origin of mailings by state**

when classifying scammer organizations since we felt the city alone was insuffiicient to positively identify a single source. But, since this information is controlled by the mailing entity (FEDEX, UPS, USPS) and not the scammer, we are confident that this information correctly geolocates individuals supporting the scammer organization.

2) Return addresses: All return addresses identified on received checks were business addresses, no personal (home) addresses were received. Figure 4 shows that 88% (29 of 33) of the check envelopes received had return addresses from 5 different states with Texas (11 checks, 8 different cities) and California (6 checks, 1 city) accounting for the majority. Of note though is that in Texas, the city the check is mailed from is the same city listed in the Return address (or at least nearby) in 89% (8 of 9) of the cases where both addresses could be identified, while in California the cities match in only 33% (2 of 6) of the checks received. Overall, where both addresses were identifiable, 41% (9 of 22) of the checks received had return addresses different than the actual city from which the check was mailed.

The three factors of the high number of discrepancies between the origin and the return addresses, all return addresses being businesses and the return address being controlled by the scammer organization results in a low confidence in the accuracy of the return address being correct and suitable for geolocation of individuals. However, if we assume the return address is fraudulent, then there is increased likelihood that checks with the same return address are from the same scammer organization and therefore we did include this datapoint in our classification strategy.

3) Business address on checks: None of the checks received had a business address that matched the return address on the envelope, with 94% (31 of 33) of the businesses from different states than the return address. Figure 5 shows the top 5 states associated with the businesses listed on the checks. While over 90% (30 of 33) of the businesses listed on the checks were identified as legitimate businesses we were unable to identify any as being complicit with the scammer organizations.

As with the return addresses, it is assumed that the address listed on the check is fraudulent and therefore unsuitable for

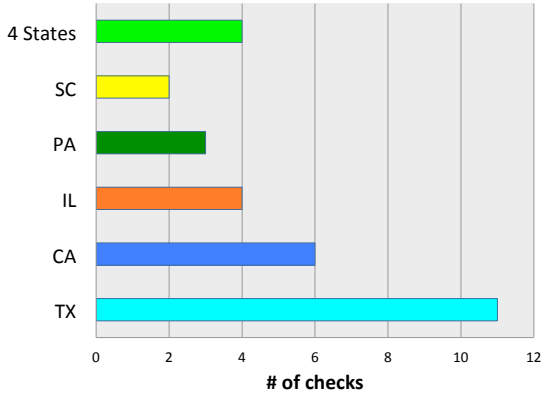

Fig. 4: **Return addresses by state**

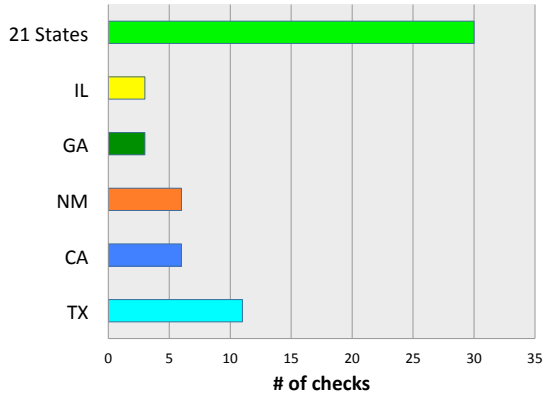

Fig. 6: **Mover agents by state**

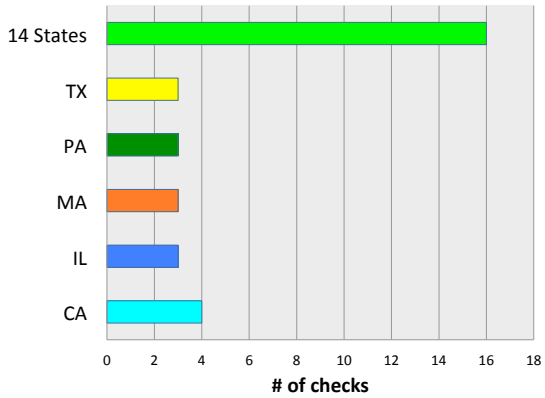

Fig. 5: **Check addresses by state**

use in geolocating scammer organizations, but the unlikelihood of multiple scammer groups using the same fraudulent business addresss means that this datapoint can be used to classify threads to a single scammer organization.

4) Bank addresses: As stated in section IV-C-1, every check had a legitimate bank address and associated routing number listed and in 73% (24 of 33) of the checks, the bank was located near the business listed on the check. The bank attempting to cash a check will not have the account information on file for the business identified on the checks, however they will be able to verify the bank address and routing number identified on the check as part of their verification process prior to disbursing money. Therefore it is necessary for the scammers to ensure that legitimate bank and routing numbers are included as part of the check. It is only upon arrival at the bank listed on the check that account information and signatures can be verified and subsequently identified as being fraudulent.

Since the majority of banks listed on checks were associated with the business addresses which were deemed likely to be fraudulent, bank addresses were also assumed to be fraudulent for use in geolocation of scammers, however, as with origin mailing addresses, bank addresses alone were deemed insufficient for categorization of scammer groups since there is a possibility of multiple scammer groups using the same bank information within large cities.

5) Mover agent addresses: Mover agent addresses are another indicator of accomplices within the United States. As with the origin address of the mailing requiring someone to print and mail the check, check scams utilizing wire transfer services such as Western Union require someone to act as a money mule and provide a layer of security between the victim and the scammer. Figure 6 shows that mover agents from 26 states were identified during this research, with the majority being used only one time for the receipt of money, although some were used up to 3 times. While it is possible that the same individual could be used both to send the check and receive the money, in only 17% (8 of 46) of the checks received where both the sender and mover agents could be identified, was the mover agent in the same vicinity as the origin of the mailing (Figure 7), suggesting that usually different individuals are used to mail out the fake checks and receive the money transfer payments. Texas again stands out as an outlier in this statistic with 63% (5 of 8) of the individuals likely to be operating as both mailer and mover agent coming from Texas.

Since the mover agent must be physically located in the city to receive funds via a money transfer service such as Western Union, this address is assessed as being sufficient for geolocation of scammers associates within the United States. Additionally since all mover agent addresses provided included street addresses as well as city/state, this datapoint is also sufficient for categorization of scammer groups.

A typical email identifying a mover agent is posted in Figure 8.

E. Fake Paypal emails

Verification that we would never accidentally receive an actual Paypal payment from a legitimate buyer was accomplished by simply never setting up Paypal accounts associated with the email accounts we used during this study. It was therefore a simple matter to identify which Paypal emails were fraudulent in their statements that money was being deposited into our (non-existent) accounts. As expected, many of the traditional

From: Owen Graig <owengraig29@gmail.com>

```
Hello, i have been informed that the check will be deliver to you today.Here is the USPS
tracking number(9405501699320017XXXXXX)I will like you to take the check to your bank and
deposit it and withdraw the out the fund.Deduct the cost of the Goods Am buying from you and
Additional $100 for your running around the have the remaining fund wire in cash by western
union to my mover today, so that as soon as they have the money, they could contact you and
Schedule a pick up time with you.The money will be wire to thier head office accountant in
Live Oak TX.... Here is their info to receive the money Via western union

Receiver's Name .. XXXXX X. XXXXX
Address .. XXXX XXXXXXX,
City .. Universal City,
State .. TX,
Zipcode .. 78148..

Transfer fee should be deducted from the money you are sending to the Mover not your own
money ..Once you have it sent, you will need to get back to me with the following details.
1 ...Senders Name: The Name you filled on the form
2 ...Senders Address: Address you filled on the form as the money sender.
3 ...Total Money Sent: Money sent after deducting the service charges
4 ...10 Digit Mtcn Number
5 ...Western Union charges.

The Movers will contact you as soon as they have the funds.I will be waiting to read from
you today.
Thank you very Much.
```

Fig. 8: **Example mover agent email.**

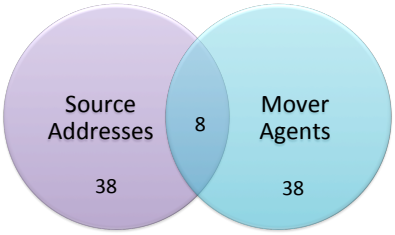

Fig. 7: **Overlap between locations of mailing origins vs. mover agents**

indicators of scam emails were present in the fraudulent Paypal emails such as misspelled words and grammatical errors, illegitimate email addresses and false company claims within the body of the email.

Fraudulent Paypal emails came in groups of three, received within a couple of minutes. The first email is a payment notification saying that the money was deposited in our account, but being held in escrow until proof of either product shipment or mover agent payment was provided. This email would have Paypal images and icons to make the notification seem as legitimate as possible.

The second email is information on the escrow procedures now being adopted by Paypal and how they are for the safety and security of both buyers and sellers. This email would also have the instructions for completing the money transfer through Western Union or other money transfer service and would have numerous references to the legitimacy of the buyer and how the process was for our safety.

The third email would be a follow-up reminder (even though it was received at the same time) to ship the product or mover agent fees and send the verification of shipment to Paypal so they could release the funds to our account. Sometimes this email would be a personal message from a Paypal representative who had been assigned to ensure completion of our money transfer.

Fake Paypal emails are constructed following scripts and use icons and graphics from legitimate sites. Therefore, content of the email bodies was not deemed sufficiently identifiable enough to categorize threads belonging to a single scammer group. Likewise, although Paypal emails did contain transaction IDs for the fake payment, these IDs were part of the email script and therefore reused among many groups.

F. Analysis of IP addresses

As described in section III-C above, we collected IP addresses from the web logs of an image host server and embedding links to product images on that server within our emails after negotiations with scammers had progressed beyond automated responses. Since our previous research collected and analyzed all IP addresses observed, for this research we focused solely on the IP geolocation for those 22 email threads for which we were able to collect both IP information and payment was attempted, either via check or

Country	Payment Method	% of IP addresses
Nigeria	Check	54.5% (12)
Nigeria	Paypal	22.7% (5)
USA	Check	0%
USA	Paypal	4.5% (1)
Other	Check	0%
Other	Paypal	18.1% (4)

TABLE IV: **IP address geolocation.**

Paypal, rather than the entire body of IP addresses.[4]

We referenced the website *whatismyipaddress.com/ip-lookup* for geolocating the IP addresses and Table IV shows that 77.2% (17 of 22) of IP addresses associated with any type of scam payments were from Nigeria with only 4.5% (1 of 22) originating from within the United States. Additionally, all of the IP addresses associated with fake check payments (12 of 12) were located within Nigeria.

V. Classification

A. Conservative Classification Strategy

We chose to continue with the conservative classification methodology used in previous research, this would allow us to compare results accurately with previous findings. Specfically, we categorized that two separate scam threads belonged to the same scammer group if they shared exactly the same email address, shipping address or phone number. However, the inclusion of the checks and associated mailing addresses accompanying them gave us additional datapoints for improving our categorization capacity including return addresses, check business addresses, check signatures and mover agent addresses. As stated previously, city/state of mailing origin and bank addresses were not deemed reliable enough to be used as stand-alone categorization datapoints to meet our conservative threshholds.

B. Top 5 groups

Resulting from our conservative classification strategy for our categorization of email threads into scammer groups, we found that the top 5 groups accounted for 56% (189 of 336) of all received scam threads (Figure 9). Table V lists additional details including the number of threads associated with each group, the number of source and reply-to email addresses, the number of different source and mover agent addresses, phone number, primary payment method and number of payments received for the top 5 groups. All of the top groups were associated with payments via fraudulent checks rather than via fraudulent Paypal payments.

VI. Lessons Learned

This work grew from proposed future works identified in a previous study of Nigerian scammers operating on Craigslist. Based upon the lessons learned from that earlier work our experiment and analysis sought to improve our methods while

[4]While this information is limited to those scammers that clicked on one of our links, we were still able to collect IPs for over 25% of all attempted fake payments.

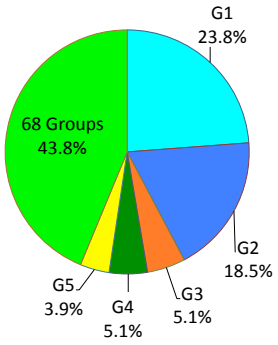

Fig. 9: **Groups by number of threads**

at the same time study a niche within the scammer community online. During this time we have identified additional challenges and improvements to our methodology. This section describe some of these lessons learned.

Our first lesson is that through the inclusion of data learned from our offline interactions with the scammers (payments via check) we were able to significantly improve our categorization of email threads into scammer groups. This enabled us to refine our groupings in not only this study but also our previous study and increase our ability to identify the top groups operating this type of scam on Craigslist. The offset to this improved capability is that conducting these offline interactions required both time and manual methods instead of the fully automated mechanisms formerly used and thereby slowed down our capability to gather and analyze data. While this reduced the quantity of data we were able to gather and analyze, the additional datapoints were critical to improving our categorization techniques and resulted in more quality assessments in the end.

Our second lesson is to discredit an assessment made regarding the lack of shipping addresses identified during a previous study [4]. The previous assessment was that 9 of the top 10 groups were more sophisticated in their ability to separate initial inquiries to postings to their scam attempts and this allowed them to keep ”clean” accounts that were not identified and blacklisted. From this study and our identification that all the top groups paid with fraudulent checks rather than Paypal, we now assess that the lack of shipping addresses derives from the fact that payment information was not shared during our previous study, so negotiations never progressed to the point where mover agents were identified. Since payments via fraudulent checks have a higher profit margin, even with the increased costs identified in Section IV-A-3, the top groups use this method moreso than the less-profitable methods such as Paypal, and therefore targeting fraudulent checks scammers may have a better payoff for law enforcement.

A third lesson is that fraudulent check collection, having them mailed to the buyer, is an effective, yet time-sensitive method. Large scammer groups are very quick to identify, and blacklist, mailing addresses for their checks. While names and email addresses were easily changed, the ability to generate

Group	# Threads	# Source Email Addresses	# Reply-To Email Addresses	Payment Method	# Payments	# Mail Sources	# Mover Agents	# Phone Numbers
1	80	35	21	Check	9	7	5	1
2	62	35	12	Check	12	9	10	5
3	17	14	7	Check	6	3	2	0
4	17	14	5	Check	5	2	3	2
5	13	11	5	Check	2	1	2	0

TABLE V: **Top 5 groups by number of threads.**

access to multiple mailing addresses, made this the chokepoint in our study and was a limiting factor on the quantity of data we gathered.

VII. Discussion and Future Work

We have presented a data focused analysis of the monetization methods used by Nigerian scammers posing as buyers targeting Craigslist. This section discusses how our analysis may be used to deter these types of scams and offer suggestions for additional work that can be undertaken to continue improving our knowledge in the future.

Top Scammer Organizations. Our categorization methods show that a small number of scammer organizations are resonsible for the majority of the scam attempts identified and provided insight into their monetization methods. We showed that the top 5 groups are responsible for over 50% of the scam payments received. This indicates that disruption efforts focusing on these top groups would have the greatest impact on the overall scammer community. As future work we plan to collect more information on identification of these top groups and the individuals associated with them along with their internal communications and structure.

Categorization Methods. We found that the addition of offline payment mechanisms and the receiving of fraudulent check payments increased our ability to identify and categorize groups of scammers. By increasing our ability to receive and analyze payments as well as further analysis of the role of the mover agent in the scam process will assist in increasing our ability to identify scammer organizations and methods as well as provide insight into the internal working and structures of the scammers. As future work we plan to design experiments to extend interactions to include the mover agents and identify their role and criticality in the scammer infrastructure.

Fake or Forged Checks. For the check we received the bank was able to verify the routing numbers, but could not verify the account numbers and signatures of the checks. As future work we plan to engage with an enforcement agency that could enable us to understand if the these parts of the check were fake or if the account numbers are valid and the check was actually a forgery that might result in funds being withdrawn from the business.

Understanding the Role of Individuals in the United States. As part of our data collection we have identified that these scammer groups have people in the United States that are either intentionally or unintentionally assisting in the monitization of these scams. As future work we plan to design a study that would enable us to contact some of these people with the goal of gaining further insights into the nature of their involvement in this ecosystem.

Links to Other Scam Operations. The identification of key, reusable datapoints uncovered during this experiment such as email addresses, phone numbers and addresses assist in the identification and categorization of scam attempts to individual scammer organizations. However these same datapoints may also be used in the identification of a scammers role in other scam communities outside of Craigslist and similar online advertisement sites. As future work we plan to analyze and look for commonalities between scammer groups identified during this experiment and those associated with scams such as dating/romance scams, spam/419 phishing scams and identity theft also traditionally associated with Nigerian scammers to further our knowledge of how scammer organizations are structured, operate and affect the larger scammer community.

VIII. Conclusion

In this paper we expanded on our previous research work presenting an empirical analysis of targeted Nigerian scams posing as buyers on Craigslist. This expanded research allowed us to improve our classification and categorization strategies and provided increased knowledge regarding the variety of patterns and methods utilized by the scammers. The continued IP address analysis confirmed that the majority of scammers are located in Nigeria, but the inclusion of the receipt of fraudulent check payments shows that the assistance of individuals within the United States is necessary to successfully implement the most popular method of these scams. The increased number of datapoints also allowed for an improved categorization strategy for identification of the large-scale scammer organizations. Finally we presented some additional discussion for future improvements and research topics for potential intervention and deterrance of this type of scam.

References

[1] Spanish Prisoner. In *Wikipedia*. Retrieved June 4, 2014, from http://en.wikipedia.org/wiki/Spanish_Prisoner

[2] Ross Anderson, Chris Barton, Ranier Bohme, Richard Clayton, Michel JG van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy*, 265-300, 2013.

[3] Monica T Whitty and Tom Buchanan. The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, 15(3): 181-183, 2012.

[4] Youngsam Park, Jackie Jones, Damon McCoy, Elaine Shi, and Markus Jakobsson. Scambaiter: understanding targeted nigerian scams on craigslist. In *NDSS*, 2014.

[5] Usman Adekunle Ojedokun and Michael Christopher Eraye. Socioeconomic lifestyles of the yahoo-boys: a study of perceptions of university students in nigeria. *International Journal of Cyber Criminology*, 6(2): 2012.

[6] Joshua Oyeniyi Aransiola and Suraj Olalekan Asindemade. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking* 14(12): 759-763, 2011.

[7] Andrew Smith. Nigerian scam e-mails and the charms of capital. *Cultural Studies*, 23(1): 27-47, 2009.

[8] Aunshul Rege, What's love got to do with it? exploring online dating scams and identity fraud. *International Journal of Cyber Criminology*, 3(2): 494-512, 2009.

[9] Cormac Herley. Why do nigerian scammers say they are from nigeria?. In *WEIS*, 2012.

[10] Dinei Florencio and Cormac Herley. Phishing and money mules. In *2010 IEEE Workshop on Information Forensics and Security (WIFS)*, 1-5, IEEE, 2010.

[11] Manny Aston, Stephen McCombie, Ben Reardon, and Paul Watters. A preliminary profiling of internet money mules: an australian perspective. In *Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*. *UIC-ATC '09*, 482-487, 2009.

[12] Tyler Moore, Richard Clayton, and Ross Anderson, The economics of online crime. *Journal of Economic Perspectives*, 23(3): 3-20, 2009.