2019

Online Deception and Situations Conducive to the Progression of Non-Payment Fraud

David Maimon
Georgia State University

Mateus Rennó Santos
University of South Florida

Youngsam Park
Yahoo Labs

Recommended Citation

Maimon, D., Santos, M., & Park, Y. (2019). Online deception and situations conducive to the progression of non-payment fraud. Journal of Crime and Justice, 42(5), 516-535.

INTRODUCTION

Online fraud is estimated to cost individuals and companies billions of dollars each year (Internet Crime Complaint Center 2017; Australian Competition and Consumer Commission 2016), and is one of the most common types of cybercrime encountered by national police agencies across the world (UN 2013). As such, several scholars and reports rate online fraud as the greatest threat to e-commerce (Jotwani and Dutta 2016; Internet Crime Complaint Center 2014). While online fraud can take different forms, including auto-fraud scams, online dating romance scams, extortion scams, and auction scams (Whitty 2013; Grabosky 2015), online non-payment and non-delivery scams have been among the most common and costly forms of online fraud during the last three years. Indeed, in both 2016 and 2017, more than 80,000 victims in the United States alone have lost more than $140 million annually to non-payment/non-delivery frauds (Internet Crime Complaint Center 2017).

Still, despite the growing public and legal interest in online fraud and in its consequences to individuals and business, the criminological literature has yet to study fraudsters' *Modus Operandi* throughout the progression of an online scam (Holt and Graves 2007; Lea, Fischer, and Evans 2009), and their responses to situational stimuli during the progression of the criminal event. To address this empirical gap, we draw on the criminal event perspective (Luckenbill 1977; Felson and Steadman 1983; Short 1998) to investigate how consistent is the use of "urgency" cues among online fraudsters when they attempt to defraud potential targets. Specifically, building on past research that focuses on fraudsters' deceptive strategies (Ferreira and Lenzini 2015; Atkins and Huang 2013), and drawing on claims from the Interpersonal Deception Theory (Buller and Burgoon 1996), we explore whether verbal and non-verbal cues of urgency are presented consistently to online fraud targets throughout the progression of an online non-payment fraud attempt. Moreover, integrating situational explanations of crime (Briar and Pilavin 1965; Osgood et al. 1996) with Buller and Burgoon's (1996) claims, we explore whether fraudsters react to the emergence of situations conducive to online fraud

by increasing the presentation of urgency cues throughout the progression of an online non-payment fraud attempt.

THEORETICAL BACKGROUND

Online fraud

With the expansion of the online environment, the Internet has become a popular medium for scams, connecting fraudsters with numerous potential targets (Pratt et al. 2010; Grabosky 2015; Reyns et al. 2016). Indeed, various types of online fraud have been developed by scammers, including sales and investment frauds (Grabosky et al. 2001), fraudulent ordering of goods (US Department of Justice 2004), auction frauds (Bailey 2009), romance scams (Whitty 2013; Whitty 2015a), and online advance fee frauds (Grabosky 2015). Among the numerous types of online frauds, non-payment and non-delivery frauds are among the most diverse (i.e., facilitated in different ways), common, and costly (Grabosky 2015; Internet Crime Complaint Center 2017).

Online non-payment frauds are scams in which goods and services are shipped to a potential buyer (consistent with the buyer's request), but payment is never received (Internet Crime Complaint Center 2017). Specifically, online fraudsters look for legitimate users' posts of "for sale" items on classified advertisement websites, and respond to legitimate ads via email or phone (Aleem and Atwi-Boasiako 2011). Once establishing the availability of a potential target, the scammer agrees to pay for the advertised product and sends a fake payment receipt (e.g. Paypal receipt) to the target (Aleem and Atwi-Boasiako 2011). If the potential target is defrauded, the victim sends out the goods to the scammer, yet receives no actual payment in return. In contrast, in an online non-delivery fraud, a payment is sent to a potential seller, but goods and services are never received (Internet Crime Complaint Center 2017). Under this type of scam, online scammers advertise an item, a real estate property, or a service over classified advertisement websites (e.g. "Craigslist.com" or "Backpage.com"), and wait for potential targets to contact them regarding the listing either over

email or phone (Button and Cross 2017). Once a potential target contacts the scammers, the online offenders push the target to send a certain amount of money for either purchasing the product or service or securing the rights to the real estate.

As in offline fraud events, fraudsters commonly employ urgency cues in their attempts to initiate online non-payment /non-delivery scams. Specifically, online fraudsters take advantage of heuristics in decision-making that are associated with peripheral processing (Johnson et al. 1993; Cowan 1986), and attempt to create a sense of urgency among potential victims by presenting very attractive offers that are presumably available only for a short time (Lea et al. 2009; Doocy et al 2001; Shichor et al. 2001). Indeed, several analyses of the content of fraudulent emails (for instance spam emails) indicate that online scammers almost always employ urgency cues during their efforts to lure potential victims into compliance (Atkins and Huang 2013; Holt and Graves 2007). Unfortunately, although this past research has advanced our understanding of the strategies used by online scammers to deceive their victims (Wang et al. 2012), these studies tend to draw on problematic samples (Ferreira et al 2015; Holt and Graves 2007), and provide no information regarding the interaction between the scammers and the victim throughout the progression of the criminal event (Atkins and Huang 2015; Ferreira and Lenzini 2015). As a result, no attention has been given to identifying the important cues that trigger offenders to pursue or abort fraud attempts. Moreover, these studies analyzed the content of unsolicited spam emails that are designed to reduce the number of replies from individuals who are unlikely to fall victim to these scams (Herley 2012). To address these empirical gaps, we explore how online fraud is perpetrated and perpetuated (Holtfreter et al. 2005), focusing on the multiple communications between online scammers and victims. To frame these communications, we adopt the criminal event perspective (Lukenbill 1977; Meier, Kennedy, and Sacco 2001) and draw on “Interpersonal Deception Theory” (Buller and Burgoon 1996) to form hypotheses regarding the role of criminal opportunities (Briar and Pilavin

1965) in conditioning the effect of initial deception displays of urgency on subsequent deceptive cues.

The Criminal Event Perspective and Interpersonal Deception Theory

The criminal event perspective focuses attention on the microsocial level of illegal behaviors, and goes beyond offenders' motivation to include insights regarding all parts of the etiology of crime, including the interaction between criminal events participants, the unfolding of criminal events, and the settings in which these events occur (Short 1998). Originating in the symbolic interactionist perspective (Goffman 1955), this approach suggests that a comprehensive explanation of crime should incorporate knowledge regarding the way offenders and victims present themselves and interact, and that the settings in which these interactions occur shape the interactive process between actors (Meier, Kennedy, and Sacco 2001). However, although advocates of the criminal event perspective believe this approach is relevant for all types of predatory crimes, prior studies employing this perspective have only focused on the interactional processes leading to violent offenses (Luckenbill 1977; Felson and Steadman 1983; Fagan and Wilkinson 1998; Deibert and Miethe 2003). Moreover, these studies do not draw on a cohesive theoretical model that allows for the development of clear research hypotheses regarding the interactions between offenders and victims, as well as the progression of the criminal event. We believe that Interpersonal Deception Theory (Buller and Burgoon 1994) can fill this theoretical void, and prove useful in understanding the interaction between fraudsters and targets during the progression of a criminal event.

The underlying premise of Interpersonal Deception Theory (Buller and Burgoon 1994, 1996; Burgoon and Buller 2015) is that social interactions involve a dynamic exchange of both verbal (i.e. linguistic and content cues (Carlson et al. 2004)) and non-verbal messages between senders and receivers, who influence each other in an interdependent fashion (White and Burgoon 2001). Deception, in this sense, occurs when a deceiver controls the presentation of information (including

the transmission of verbal and non-verbal messages, as well as the manipulation of situational cues) in an effort to change a target's beliefs in a way that the deceiver knows is dishonest (Buller and Burgoon 1994). According to Buller and Burgoon (1994; 1996), deceptive communication is similar to normative communication, since it requires active participation from both the deceiver and the target, and since it involves the presentation of both strategic and non-strategic behaviors (Goffman 1969). Non-strategic behaviors are unintentional and unconscious actions that are presented by a sender during the progression of an interaction. Strategic behaviors, on the other hand, are purposive actions that involve intentionality and conscious awareness. Buller and Burgoon (1996) contended that since deceivers engage in activities designed to manage information, behavior, and image, they are more likely to display strategic behaviors than truth tellers[1] (Burgoon, Proudfoot, Schuetzler, and Wilson 2014). However, to increase their credibility and evade detection, deceivers accept feedback regarding their own performance from those they interact with (i.e. their potential victims), and react to signs of suspicion by modifying their behaviors accordingly (see also Goffman 1955).

Interpersonal Deception Theory and The Online Environment

Although several studies investigated the way in which initial deception cues shape deceivers' behaviors along the progression of deceptive interactions in an *offline environment* (Burgoon, Buller, White, Afifi, and Buslig 1999; White and Burgoon 2001), only scant research has been devoted to how *computer mediated environments* influence communication patterns between deceivers and targets throughout the progression of online criminal events (Pak and Zhou 2014). This is unfortunate because several scholars believe that the low level of context interactivity facilitated by computing environments provides fertile ground for norm breaking and deception. Carlson and associates (2004) argued that low interactivity communication platforms like email and text messaging support the development of deceptive behavior by allowing communicators to monitor only a few communication channels, and consequently simplify offenders' efforts to synchronize and coordinate

the social cues they transmit over these channels. In contrast, other scholars believe that although non-verbal cues such as facial expression (Goffman 1955) and vocal pitch cannot be transmitted over a text-based interaction, other non-verbal cues can be transmitted to convey senders' feelings and emotions (Kotlyar and Ariely 2013). For example, Byron and Bladrige (2007) showed that emails written in all capital letters could convey senders' feelings of anger and urgency. Similarly, Kalman and Gergle (2014) demonstrated that letter repetition as an extension of a word (e.g. "sooo" and "thaaanks") is used to convey emotional nuance.

In line with the growing arguments that computer-mediated communications can transfer both verbal and non-verbal social cues, numerous studies have investigated the relationships between verbal and non-verbal cues and different types of online deception (Pak and Zhou 2014; Hauch, Blandon-Gitlin, Masip, and Sporer 2015). In general, most of these studies found that certain verbal and non-verbal communication cues are associated with deceptive behaviors. For example, Ho and colleagues (2015) reported that online deceivers are more likely to avoid using the words "no" and "not" while interacting with other online users than truth-tellers. Similarly, Derrick and colleagues (2013) found that deceivers had longer response latencies when interacting with online users over chat-based platforms than truth-tellers.

Despite this research, only a few studies have focused on the interactive exchanges between deceivers and targets, and even less research has investigated how deceivers' initial presentation of deceptive behaviors is correlated with their subsequent behaviors during the progression of the online crime (Pak and Zhou 2014). Moreover, only a few of these studies collected data from online users while preserving the context in which deceit takes place (Kotlyar and Ariely 2013), and none of them analyzed data collected from online criminals. Similarly, no previous study has tested how fraudsters identify criminal opportunities through the presentation of deception cues in general, and urgency cues in particular, during the progression of offline or online criminal events. We suspect that the

identification of a criminal opportunity could influence offenders' situational motivation to pursue a criminal event (Briar and Piliavin 1965), and shape offenders' presentations of both verbal and nonverbal deceptive cues throughout the progression of the online criminal event.

Offline and Online Situations Conducive to Crime

The role of environmental factors in determining both motivational and situational opportunities to offend has been discussed extensively in criminological scholarship during the last five decades (Briar and Piliavin 1965; Clarke 1997). Briar and Piliavin (1965) contended that exposure to situationally induced stimuli may shape individuals' morals and behaviors and, in turn, that an individual's engagement in a criminal event is the result of situational motivations to offend. More recently, Osgood and colleagues (1996) have expanded Briar and Piliavin (1965) claims to account for individual offending and violent behaviors among adolescents and youths. Specifically, integrating Briar and Piliavin's (1965) situational conception of delinquent motivation with Cohen and Felson's (1979) emphasis on individuals' daily routines, Osgood and associates (1996) argued that situations in which deviance is easier and rewarding are likely to increase the probability of deviant behavior and crime. While Osgood and colleagues (1996) identified unique criminogenic situations under which juvenile delinquency is likely to ensue (i.e. unstructured socializing with peers), several scholars have acknowledged the role of criminal opportunities for the development of fraudulent behaviors. Roberds (1998) suggested that situations in which buyers and sellers do not have an ongoing business relationship, as well as those in which the payer's identity cannot be traced, increase the likelihood of fraud. Moreover, Roberds (1998) contended that situations in which a seller cannot withhold delivery of an item until the buyer pays in full, and the payment is verified, increase the probability of fraud. Finally, Osgood and colleagues (1996) acknowledged the role of availability in the context of income tax fraud, noting that "income tax is impossible without earnings that are subject to taxation" (639).

Indeed, several studies have previously emphasized the role of target availability and suitability in increasing offenders' situational motivations to offend, and in influencing the likelihood of a criminal event to occur (Cohen and Felson 1979; Wright and Decker 1994, 2011). Wright and Decker (1994) reported that burglars prefer to target residential houses that appear to host valuable items over houses that appear easy to break into. These scholars also observed that when seeking potential robbery targets, robbers attempt to confirm that the targets carry plenty of cash before initiating the criminal event (Wright and Decker 2011). Unfortunately, only scant research has tested the relationships between online situations conducive to crime and online offending. In fact, we were able to find only one study (Ingram and Hinduja 2008) that emphasized the role of availability of online targets as a key online situation that increases motivations to engage in crime. Specifically, Ingram and Hinduja (2008) reported that the availability and accessibility of pirated material in the online environment increased undergraduate students' probability to engage in copyright infringement. Still, consistent with the underlying premise of situational explanations of crime (Briar and Piliavin 1965; Clarke 1997; Eck and Clarke 2003), and with Wright and Decker's (1994, 2011) findings, our work seeks to assess the role of situations conducive to online fraud, and specifically of confirmed target suitability, in shaping online fraudsters' deceptive behaviors during the progression of an online advance fee fraud attempt.

The current study

Since many online scammers employ verbal messages of urgency when contacting their victims with different fraudulent propositions (Atkins and Huang 2013; Wang et al. 2012), we first aim to assess how consistent the presentation of verbal cues of urgency is throughout the progression of an online non-payment fraud attempt. Adopting Goffman's (1955) claim that inconsistency in how a person projects himself in society risks embarrassment and discrediting by others, we suspect that in the absence of suspicion signs among their targets, deceivers are likely to display consistent strategic

behaviors (Buller and Burgoon 1996). In this sense, we suspect that online scammers who incorporate verbal cues of urgency in their initial interactions with victims are likely to employ subsequent verbal cues of urgency along the progression of the online fraud attempt. Thus, our first research hypothesis suggests that *verbal cues of urgency are more likely to appear in follow-up communications with online fraudsters who incorporated verbal cues of urgency in their initial communication with a target, compared to follow-up communications from online fraudsters who did not incorporate verbal cues of urgency in their initial communications with targets.*

Relatedly, drawing on Buller and Burgoon's (1996) assumption that deceivers accept feedback regarding their own performance from their targets and adjust their behaviors accordingly, we suspect that upon receiving clear signs of target suitability and online opportunities to defraud, online scammers believe that the targets have accepted their façade and are ready to comply with the scammers' requests. In order to present consistency in their strategic behaviors and avoid raising suspicion, the scammers will likely continue using verbal messages that they used in previous interactions with their targets. Therefore, our second hypothesis suggests that *confirming target suitability will increase the probability of verbal cues of urgency in follow-up communications with online fraudsters who incorporated verbal cues of urgency in their initial probe, compared to when a feedback regarding target suitability is missing.*

Consistent with the assumption that deceivers employ both verbal and non-verbal deceptive cues during their interaction with victims, we also seek to discover whether initial verbal cues of urgency are synchronized with subsequent non-verbal cues. Specifically, in line with the assumption that computer-mediated environments could support the transmission of nonverbal cues (Derrick et al. 2013), we believe that online scammers may support the urgency façade they are trying to present to their targets by communicating non-verbal cues of urgency. One type of nonverbal cue of urgency that is commonly employed by telemarketing fraudsters to create a sense of urgency among their

victims involves increasing the number of contacts with a target (Shichor et al. 2001). Similarly, we suspect that online scammers who attempt to create a sense of urgency among their targets will increase the frequency of their online contact (through emails, IM, etc.) with victims. Thus, our third research hypothesis suggests that the *frequency of repeated communications between scammers who incorporate verbal cues of urgency in their initial contact with targets will be higher than the frequency of repeated communications between online scammers who do not incorporate initial verbal cues of urgency in their initial contact with targets.*

Finally, we suspect that confirmation of target suitability may enhance the effect of initial verbal cues of urgency on the frequency of email communication between online scammers who employ verbal cues of urgency and potential targets. Specifically, it is possible that targets' willingness to share details about the availability of situations conducive to crime will be interpreted by online scammers as a sign of the target's willingness to comply without expressing suspicion. As such, the online scammers who employ verbal cues of urgency may believe that there is no need for them to modify their strategic behaviors (Buller and Burgoon 1996), and instead, may introduce subsequent non-verbal cues of urgency that coincide with the urgency façade. Therefore, our final research hypothesis suggests that *the frequency of repeated communications with online scammers will be higher when feedback regarding the availability of suitable target is received by scammers who incorporate verbal cues of urgency in their initial contact with a target, compared to when a feedback regarding target suitability is missing.*

DATA AND METHODS

In order to provide a clear understanding of the sequence of events during the progression of online fraud, we followed Deibert and Miethe's (2003) approach and initiated the collection of processual data (i.e. data that provides clear temporal sequencing of actions during the progression of a criminal event) on online non-payment fraud attempts while engaging with the users of an online classified

advertisement website.

Procedure

Drawing on Kshetri's (2010) claim that geographic locations play important role in determining targets attractiveness to online fraud activities, we selected 10 large metropolitan areas (San Francisco, Seattle, New York, Boston, LA, San Diego, Portland , Washington DC, Chicago, and Denver) and 10 small towns (Twin Tiers, Cumberland Valley, Meadville, Susanville, Siskiyou, Hanford-Corcoran, Santa Maria, Winchester, Southwest, and Eastern Colorado) in the U.S.A., where we advertised the sale of four types of products– cell phones, computers, jewelry, and auto parts– over the classified advertisement webpages that are designated for serving these locations. Our decision to advertise our items in both large metropolitans and small towns draws on past research's findings suggesting that residents in small towns with low shop accessibility buy and sell products more often online (Farag et al 2006), and consequently, may be more susceptible to online fraud activities. Each ad included information on a single item, and the requested price for it. Items' prices ranged from $110 to $700. Examples of the type of advertisements we posted under each product category are presented in Appendix A, Panel A. We decided to post advertisements for these specific products since we found that these items were popular at Amazon.com. The prices we asked for in our advertisements for used products were substantially higher than the prices advertised for identical yet new products on Amazon.com (Alem and Atwi-Boasiako 2011). Our decision to overprice our items was driven by a "Scam Alert" posted by the Federal Trade Commission's Consumer Protection Team, which indicated that online fraudsters respond to "for sale" ads independent of the seller asking price, while legitimate online consumers are reluctant to reply to posts of overpriced products (Tuscan 2014).

In order to minimize potential biases in our data collection, we programmed our servers to post the advertisements in an evenly distributed rate across posting times and product categories.

Specifically, we posted our ads at a low rate[2] of one advertisement per category per city, every 48 hours (Park et al. 2014). By the end of the three-month experimental period (from 4/15/2013 to 7/19/2013), we had posted 1,376 advertisements on the local classified advertisement websites of the 20 selected cities. However, since 747 of these advertisements were flagged and deleted by the classified advertisement website team, only 629 of the advertisements (an average of 157.3 ads per product category) remained posted until they expired (typically after 7 days)[3].

To enable an email exchange with potential online consumers, we opened 42 new email accounts,[4] periodically checked the 42 inboxes, identified responses to our advertisement, and replied to all incoming emails with a subject line that directly referenced the subject of our post. To simplify this process, we looked for a list of eight keywords in the email received in our 42 email inboxes, and once identifying one or more of these words, generated a predetermined and consistent response that adequately reacted to each word. For instance, once we identified the word "price" in the potential online consumer's email, we generated the following response: "The price is X, firm." Similarly, if a potential online consumer asked about the advertised item's condition in his probe email, we generated the following response: "The condition is almost perfect since it was not used frequently." When multiple words were identified in a single communication, we combined multiple sentences in a single response. If we identified none of the keywords, no response was sent to the potential online consumer. Appendix A, Panel B presents the list of keywords we searched in the emails and the corresponding response we generated to each of these words. The consistent responses we generated allowed us to exchange multiple rounds of emails with potential online fraudsters. Appendix B, Panel A presents an example of a typical exchange our team had with online fraudsters. The communication between the research team and an interested online consumer/fraudster was terminated if the potential online consumer/fraudster did not respond to our email or if none of the key words which triggered the research team's response appeared in the email we received.

Importantly, our research design was approved by the IRB committee in the University of Maryland.

Sample

We received a total of 19,204 emails in our 42 email accounts during the experimental period. Of these, 13,215 emails were initial probe emails sent to us by potential online consumers who were interested in the items we advertised. The remaining emails received in our inboxes were mainly spam emails and emails sent from email service providers (e.g. Gmail and Yahoo). From the 13,215 scam-related first responses, we identified 8,048 emails with a subject line that replied directly to the subject of our post, searched the email body for the relevant keywords, and sent first replies to the online consumers. By sending a reply to the online consumers, an email thread was automatically generated in our email inboxes.

We received at least one unique response to 1,140 of the email responses we sent in reply to inquiries about our ads. Importantly, during our communication with the interested online customers we received 623 unique emails (making 623 unique email threads) with fake PayPal payment notifications stating that funds were transferred to our PayPal account, followed by a request for us to send the relevant product to the consumer's mailing address. Since none of the PayPal payment confirmation emails arrived from legitimate PayPal email accounts, and since we never set-up PayPal accounts for this project, the fake receipts constitute strong evidence that those emails were sent by *online fraudsters*. In contrast, the other 517 email threads did not include neither fake payment notification, nor other signs of fraudulent activity. Therefore, one may suggest that these emails were sent by legitimate potential online consumers. Since the focus of this paper is on online fraudsters' deceptive cues, our final sample consists of the 623 email threads that included that fake PayPal notifications and that were certainly sent by online fraudsters.

Dependent measures

The unit of analysis in this work is the email thread (i.e. an email message that includes a running list of all the succeeding replies, starting with the original email), which encompasses the progression of an online non-payment fraud attempt event. To test our first and second research hypotheses, we constructed the measure *subsequent verbal cues of urgency*. Specifically, drawing on the rationale proposed by the "Manifest Content Analysis" approach (Maruna 2010) and its implementation in the criminological field (Welch, Fenwick and Roberts 1998), and consistent with the technical operation of several existing email filters that are designed to identify and classify email urgency (Horvitz and Apacible 2009), we identified the urgency words "ASAP," "soon," and "fast" in email messages we received from online fraudsters who responded to our conversation engine, and created a dummy variable indicating the presence of at least one of these words in the email message. Importantly, the three urgency-keywords we used for constructing this dependent variable are used by bulk-filters to identify, flag, and classify email messages for urgency and importance (Horvitz and Apacible 2009).

To investigate our third and fourth research hypotheses we created the measure *subsequent non-verbal cues of urgency*. Following Shichor and colleagues' (2001) conceptualization of non-verbal cues of urgency, this measure is a simple count of the number of email responses we received from online scammers regarding the items we advertised. Consistent with Shichor et al. (2001), we associate a higher number of emails from a unique online scammer during a unique interaction regarding a product we advertised as a non-verbal cue of urgency.

Key independent measures

To investigate whether initial presentation of urgency cues determine the presentation of both non-verbal and verbal cues of urgency throughout the progression of online non-payment fraud attempts, we identified emails received in our email inboxes from potential online scammers that contained at least one of the three urgency keywords. Specifically, in line with the operation of Horvitz and Apacible's (2009) bulk-email filter, we identified the urgency words "ASAP," "soon," and "fast" in

the first emails messages we received from online fraudsters to construct the measure *initial verbal cues of urgency* (1= at least one urgency word is present in the scammer's first email).

To assess how the discovery of target suitability and situations conducive to online fraud influences the presentation of deception cues throughout the progression of the online criminal event, we distinguished between probe emails that requested information regarding the condition of the advertised item and probe emails that did not, and used those probes to construct our measure for *confirmation of target suitability.* Specifically, if the online scammers asked about the advertised item condition in his probe email, we sent the following response: "The condition is almost perfect since it was not used frequently." In the absence of this keyword in the probe email, we did not disclose any information about the item's condition. Appendix B, Panel B presents examples of probe emails that received confirmation of target suitability, and of probe emails that did not receive such a response. Thus, the measure we generated is a binary variable indicating whether or not we sent potential fraudsters explicit confirmation regarding the item condition (1=information regarding item condition was sent to scammers).

Control variables

We used a list of measures designed to control for potential influences of the ad's content on online scammers' probability to consistently pursue both verbal and non-verbal cues of urgency. We generated a list of dummy variables to indicate whether the posted ad offered an *auto part*, a *cellphone*, a *computer*, or *jewelry* for sale. The *price* is a measure of the asking price (in U.S. dollars) of the item advertised. Finally, since we posted our advertisements in both major metropolitan areas and small towns, we composed the dummy variable *major metropolitan* to indicate the location in which the ad was posted (1= major metropolitan). Means and standard deviations for all the dependent and independent variables are reported in Table 1.

[TABLE 1 HERE]

Analytic strategy

To assess the direct and interactive effects of initial verbal cues of urgency and confirmation of target suitability on our first dependent measure (i.e. subsequent verbal cues of urgency), we estimated a series of logistic regressions (Long 1997). Due to the positively skewed distribution of our email contacts count measure, as well as an observed overdispersion when estimating a simple Poisson model, we employed a series of negative binomial regression models (Osgood 2000), to estimate the direct and interactive effects of initial verbal cues of urgency and confirmation of target suitability on the number of emails we received from online scammers (i.e. non-verbal cues or scarcity).

RESULTS

Before investigating our key research hypotheses, we briefly describe our unique sample characteristics. As presented in Table 1, the most common email thread that was initiated by an online scammer was initiated in response to the jewelry ads we posted on the classified ad website (36%), followed by computer ads (28%), cellphone ads (24%), and auto-part ads (12%). Importantly, 18% of the scammers' probe emails included specific words that are aimed to convey a sense of urgency on behalf of the scammer, while 20% of the initial probe emails received a confirmation of target suitability from our research team. Finally, the average number of subsequent email responses we received during our online engagement with online fraudsters was 2.59 emails, while 70% of the subsequent emails we received included urgency words.

Turning to our first research hypothesis, we next present findings from a Logit model that estimates the effect of initial verbal cues of urgency on the probability of subsequent verbal cues of urgency in follow-up email communications between the online scammers and our research team. Results from this analysis are presented in Table 2, Model 1. As indicates in the model, scammers' presentations of verbal cues of urgency in the probe email increases the odds ratio for the appearance

of verbal cues of urgency in subsequent email communications between the online scammers and our team. However, this effect is only marginally significant ($p < 0.1$).

To test our second research hypothesis, we specify an interaction term between initial verbal cues of urgency and confirmation of target suitability, and estimate its effect on the probability that subsequent verbal cues of urgency will be presented by online scammers during the progression of an online non-payment fraud attempt. Findings from this analysis are reported in Table 2, Model 2. As indicated in the model, the interaction between confirmation of target suitability and initial verbal cues of scarcity is significant and positive, suggesting that confirmation of target suitability enhances the effect of initial verbal cues of urgency on subsequent presentation of verbal cues of urgency.

Next, we re-estimate Model 2 while introducing the list of controls and accounting for their potential confounding effects on both the dependent and independent variables. Findings from this model are reported in Table 2, Model 3. As indicated in the model, the effects of none of these controls is significant on subsequent presentation of verbal cues of urgency. However, the effect of the interaction between initial verbal cues of urgency and confirmation of target suitability remains significant. Notably though this model presents a relatively low pseudo R-squared value. Indeed, the relatively low pseudo R-squared value may be a reason for concern in these models. However, it should be noted that the only true utility of pseudo R-squared in non-parametric model is in comparing the Pseudo R-squared values against other pseudo R-squared values of the same type, generated from the same data, on the same outcome (Long & Freeze, 2006). Much like pseudo R-Squared values, Akaike Information Criterion (AIC) values could also be calculated in order to estimate which model is more parsimonious, and fits the data better. Both the pseudo R-squared and AIC values reported for these models suggest that Model 3 represent a substantial improvement over both Model 1 and Model 2, and that the effect of this interaction term is not trivial in the model.

[TABLE 2 HERE]

To visualize the magnitude of this effect we plot in Figure 1 the predicted probability of subsequent verbal cues of urgency for online scammers who either incorporated urgency verbal cues in their probe email or did not, and who either received a confirmation of target suitability or did not. As indicated in the figure, the predicted probability of verbal cues of urgency in subsequent communication between online fraudsters and our research team ranges between 63% and 67% when scammers are not presented with confirmation of target suitability. However, the predicted probability of subsequent verbal cues of urgency is 89% when confirmation of target suitability is presented in response to probe emails with urgency words. In contrast, the predicted probability of subsequent verbal cues of urgency is 61% when confirmation of target suitability is presented in response to probe emails with no urgency words.

[FIGURE 1 HERE]

To test our third research hypothesis and assess whether the presentation of verbal cues of urgency is synchronized with non-verbal cues of urgency throughout the progression of an online non-payment fraud attempt, we estimated the effect of initial verbal cues of urgency on the number of follow-up email communications between online scammers and our research team, using a Negative Binomial Regression. Results from this analysis are presented in Table 3, Model 1. As indicated in the model, the effect of scammers' presentation of verbal cues of urgency in the probe email is significant and positive, suggesting that the presence of initial verbal cues of urgency significantly increases the frequency of email communication between online scammers and the research team.

Next, we estimate the effect of the interaction term between verbal cues of urgency and confirmation of target suitability on the number of follow-up email communications between online scammers and our conversation engine. Findings from this analysis are reported in Table 3, Model 2. In line with the findings reported when predicting subsequent verbal cues of urgency, the effect of the interaction between verbal cues of urgency and confirmation of target suitability is significant and

positive on the number of email communications between online scammers and the conversation engine. This finding supports the assumption that confirmation of target suitability enhances the effect of initial verbal cues of urgency on subsequent presentation of non-verbal cues of urgency.

Finally, we re-run the model while introducing the list of controls and accounting for potential confounding effects on both the dependent and independent variables. Findings from this model are reported in Table 3, Model 3. Note that the effects of cellphone, computers, and jewelry ads are significant and positive in the model. In contrast, the effect of major metropolitan measure is significant and negative. Still, the effect of the interaction term between initial verbal cues of urgency and confirmation of target suitability remains significant in the model, suggesting that the interactive effect is not trivial. Moreover, both the pseudo R-squared and AIC values reported for these models suggest that Model 3 represent a substantial improvement over both Model 1 and Model 2.

[TABLE 3 HERE]

To visualize the magnitude of this effect, in Figure 2 we plot the predicted number of email communications between online scammers and the research team for online scammers who either incorporated urgency verbal cues in their probe email or did not, and for scammers who either received a confirmation of target suitability or did not. As indicated in the figure, the predicted number of email communications between online scammers and the research team is 2.3 emails on average when scammers are not presented with confirmation of target suitability. However, the predicted number of email communications between online scammers and the research team is 3.6 emails when confirmation of target suitability is presented in response to probe emails with urgency words. In contrast, the predicted number of email communications between online scammers and the research team is only 1.9 emails when confirmation of target suitability is presented in response to probe emails with no urgency words.

[FIGURE 2 HERE]

Sensitivity analysis

Although the findings presented so far support our research hypotheses, one may suggests that by focusing our analyses on the 623 email threads in which we received a fake payment notification only, it is impossible to discern whether the observed patterns are unique to online offenders. Indeed, it could be the case that legitimate online consumers who are in a rush to purchase an item online adopt a similar strategy to that we observed among online fraudsters. Therefore, ideally, our assessments of the four research hypotheses should also include an exploration of the way potential online consumers (i.e. non-fraudsters) employ both verbal and non-verbal cues of urgency during their interactions with online sellers. In order to address this issue, we re-estimated all the models we reported above using data from the 517 email threads that did not include a fraudulent payment notification. Since none of these email-threads included concrete evidence for an online fraud attempt, we suspect that these email communications may have been with legitimate online consumers who were genuinely interested in purchasing the advertised items. Results from these analyses (see Appendix C for the findings from all re-estimated models) reveal that none of the verbal and non-verbal consistencies of urgency we observed among online-fraudsters are evident among non-fraudsters. Moreover, confirmation of item availability does not moderate the effect of initial verbal cues of urgency on subsequent verbal and non-verbal cues of urgency.

[TABLE 4 HERE]

DISCUSSION

Despite the growing public and legal interest in online fraud, and the potential of the social sciences to guide both technical and policy efforts to prevent and mitigate this phenomenon, relatively little attention has been given in the criminological literature to investigating fraudsters' *Modus Operandi* (Lea et al 2009), and their responses to situational stimuli during the progression of these criminal events. To bridge this empirical gap we adopted the criminal event perspective (Meier et al 2001),

and drew on claims from the Interpersonal Deception Theory (Buller and Burgoon 1996) to explore whether verbal and non-verbal cues of urgency are presented consistently to online-fraud targets throughout the progression of an online non-payment fraud attempt. Moreover, integrating Buller and Burgoon's (1996) claims with situational explanations of crime (Briar and Pilavin 1965; Osgood et al. 1996), we explored whether the confirmation that a situation is conducive to online fraud impacts the presentation of urgency cues throughout the progression of an online non-payment fraud attempt. Analyzing data collected through unique email communications between online fraudsters and our research team revealed several key findings.

First, in contrast to previous research that analyzed the content of spam emails and reported that many online scammers employ verbal cues of urgency when contacting their victims with different fraudulent propositions (Wang et al. 2012), we find that verbal cues of urgency in initial probe emails sent to potential targets of non-payment fraud are relatively rare, with only 18% of the probe emails received in our email inboxes incorporating verbal cues of urgency like "fast," "soon," and "ASAP." Similarly, only 20% of the probe emails actively sought to confirm the target's suitability by attempting to gather intelligence about the target condition and functionality. Future research should explore how common the use of other persuasive approaches (for example authority, social proof, and liking (Ferreria and Lezini 2015)) is in the context of online fraud in general, and in non-payment/non-delivery fraud attempts in particular.

Second, we find some evidence that verbal cues of urgency are more likely to be incorporated in fraudsters' subsequent emails to targets if verbal cues of urgency were included in the fraudster's initial probe email, compared to threads where such cues were absent from the initial probe. Moreover, we find that confirmation of target suitability increases online fraudsters' consistent use of verbal cues of urgency throughout the progression of the online fraud attempt, if the initial probe email included verbal cues of urgency. These first of its kind "context-embedded" findings support

Buller and Burgoon's (1996) suggestion that in the absence of clear signs of suspicion from targets, deceivers are likely to display consistent strategic online behaviors throughout the progression of online fraud. However, the estimated model fit values calculated for these models suggest that these findings should be interpreted cautiously.

Third, consistent with the assumption that fraudsters employ both verbal and non-verbal deceptive cues during their interactions with victims, we observed that the volume of email messages sent to potential targets is significantly higher among scammers who incorporated verbal cues of urgency in their probe emails, compared to scammers who did not incorporate initial verbal cues of urgency in their probe emails. This pattern is consistent with the pattern observed by Shichor and associates (2001) in the context of telemarketing fraudsters, and offers support to the suggestion that computer-mediated environments could support the transmission of nonverbal cues in general (Derrick et al. 2013) and the transmission of non-verbal urgency cues in particular.

Finally, we found supporting evidence for our last research hypothesis, suggesting that the confirmation of target suitability enhances the effect of initial verbal cues of urgency on the frequency of email communication between online scammers who employ verbal cues of urgency and potential targets. Specifically, we reported that the confirmation of target suitability increases the volume of email messages sent to potential targets by online fraudsters if the initial probe email included verbal cues of urgency. Indeed, we believe that targets' willingness to share details about the availability of situations conducive to crime is perceived by online scammers as a sign of compliance, and results in subsequent presentation of non-verbal cues of urgency that coincide with the urgency façade (Buller and Burgoon 1996).

The findings reported in our paper emphasize the relevance of the criminal event perspective in understanding the dynamics of online fraud, and expand the body of criminological literature that has already investigated key insights from this perspective in the context of violent crime (Luckenbill

1977; Meier et al. 2001). Moreover, our seminal findings demonstrate the importance of situations conducive to online fraud for determining offenders' presentation of deceptive cues while attempting to defraud their victims. Future research should further explore how the emergence of situations conducive to online crime dictates the presentation of other known deceptive cues (for instance, authority and kindness (Ferreria and Lezini 2015)) throughout the progression of an online fraud. We suspect that such future work should further apply insights from Buller and Burgoon's (1994, 1996) Interpersonal Deception Theory. In parallel, we believe that efforts should be devoted to the development of a more comprehensive criminological theory that can investigate and predict the progression of a criminal event.

Besides the important theoretical contribution of this research to the criminological literature, we believe that this work also carries practical implications for spam filter designers and organizations that attempt to detect and prevent online fraud victimization. Specifically, we know that email providers consistently calibrate their spam filters to try and prevent spam emails from ending up in email users' inboxes. Unfortunately, these spam filters do not completely prevent spam email from arriving to potential targets (Jakobson and Leedy 2016). The approach we bring paves a path for the design of new tools that could monitor the series of interactions occurring during the progression of a criminal event in effort to detect, flag, and block them from result in victimization.

Still, this work is not without limitations. First, in many instances the classified ad website flagged and deleted our advertisements from their servers. Although we were unable to identify a systematic reason as to why some advertisements were removed, we have no reason to believe that this issue impacted the results obtained, as scammers were presumably as likely to respond and to use urgency cues for these ads as for any others. Second, we did not initiate contact with potential consumers and scammers who did not have the ad's subject line in the header. Relatedly, although the key words we choose as a trigger for response appeared frequently in both a pilot study we

conducted, as well as used by other scholars to set email filters (Horvitz and Apacible 2009), future research should investigate whether responses to other words change online fraudsters' responses, and the progression of an online fraud event. Finally, we cannot really identify the individuals who contacted us throughout the data collection period, and assess their demographic characteristics (Button and Cross 2017), personality traits (Holtfreter, Reisig, and Pratt 2008), or motivations behinds their responses to our advertisements. Collecting such data could have improved our models' predictability. Moreover, we cannot determine with a very high level of confidence if the exchanges we had over 1,140 email responses were with unique or overlapping online consumers/scammers. However, we believe that since the unit of analysis in this work is the progression of a criminal event this generate less of an issue[5]. Therefore, despite these limitations, we believe that this paper contributes to our understanding of the development of online fraud events, and provides additional evidence for the promise embedded in criminological research for guiding the detection, mitigation, and prevention of online crimes.

REFERENCES

Aleem, A., and Antwi-Boasiako, A. (2011). "Internet auction fraud: The evolving nature of online auctions criminality and the mitigating framework to address the threat." *International Journal of Law, Crime and Justice* 39 (3): 140-160.

Atkins, B., and Huang, W. (2013). "A study of social engineering in online frauds". *Open Journal of Social Sciences*, *1*(03), 23.

Australian Competition and Consumer Commission. (2016). *Targeting Scams: Report of The ACCC on Scams Activity 2015*. Available at: https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scam%20activity%202015.pdf

Bailey, S. (2009). "Fighting an Anonymous Enemy: The Uncertainty of Auction Sites in the Face of Tiffany v. eBay and LVMH v. eBay." *California Western International Law Journal* 40: 129.

Briar, S., and Piliavin, I. (1965). "Delinquency, situational inducements, and commitment to conformity." *Social Problems* 13: 35.

Buller, DB., and Burgoon, JK. (1994). "Deception: Strategic and nonstrategic communication." *Strategic interpersonal communication* 191-223.

Buller, DB., and Burgoon, JK. (1996). "Interpersonal deception theory." *Communication theory* 6(3): 203-242.

Burgoon, JK., and Buller, DB. (2015). "Interpersonal deception theory: Purposive and interdependent behavior during deceptive interpersonal interactions." *Engaging theories in interpersonal communication, 2e*: 349-362.

Burgoon, JK., Proudfoot, JG., Schuetzler,R., and Wilson, D. (2014). "Patterns of nonverbal behavior associated with truth and deception: Illustrations from three experiments." *Journal of Nonverbal Behavior* 38(3): 325-354.

Burgoon, JK., Buller, DB., White, CH., Afifi, W., and Buslig, ALS. (1999). "The role of conversational involvement in deceptive interpersonal interactions." *Personality and Social Psychology Bulletin* 25(6): 669-686.

Button, M., and Cross, C. (2017). Cyber Frauds, Scams and their Victims. Routledge: Taylor and Francis Group.

Carlson, JR., George,JF., Burgoon, JK., Adkins, M., and White, CH. (2004). "Deception in computer-mediated communication." *Group decision and negotiation* 13(1): 5-28.

Chang, JS, and David MC. (2010). "Psychological influences in e-mail fraud." *Journal of Financial Crime* 17 (3): 337-350.

Clarke, R. (1997). *Situational crime prevention*. Monsey, NY: Criminal Justice Press.

Cohen, LE., and Felson, M.(1979). "Social change and crime rate trends: A routine activity approach." *American sociological review* : 588-608.

Cowan, DA. (1986)."Developing a process model of problem recognition." *Academy of Management Review* 11(4): 763-776.

Cross, C., and Blackshaw, D. (2015)."Improving the police response to online fraud." *Policing* 9(2): 119-128.

Deibert, GR., and Miethe, TD. (2003). "Character contests and dispute-related offenses." *Deviant Behavior* 24 (3): 245-267.

Derrick, DC., Meservy, TO., Jenkins, JL., Burgoon, JK., and Nunamaker., JF. (2013). "Detecting deceptive chat-based communication using typing behavior and message cues." *ACM Transactions on Management Information Systems (TMIS)* 4(2): 9.

Doocy, JH., Shichor, D., Sechrest, DK and Geis, G. (2001)."Telemarketing fraud: Who are the tricksters and what makes them trick?." *Security Journal* 14 (3): 7-26.

Fagan, J., and Wilkinson, DL. (1998). "Guns, youth violence, and social identity in inner cities." *Crime and justice* 24: 105-188.

Farag, S., Weltevreden, J., Rietbergen, TV., Dijst, M., and van Oort, F. (2006). "E-shopping in the Netherlands: does geography matter?." *Environment and Planning B: Planning and Design* 33, (1) : 59-74.

Felson, RB., and Tedeschi, JT. (1993). "A social interactionist approach to violence: Cross-cultural applications." *Violence and victims* 8(3): 295-310.

Felson, RB., and Steadman, HJ. (1983). "Situational factors in disputes leading to criminal violence." *Criminology* 21(1): 59-74.

Ferreira, A., and Lenzini, G. (2015). "Can Transparency Enhancing Tools Support Patient's Accessing Electronic Health Records?." In *New Contributions in Information Systems and Technologies*, pp. 1121-1132. Springer International Publishing.

Goffman, E. (1955). "On face-work: An analysis of ritual elements in social interaction." *Psychiatry* 18(3): 213-231.

Goffman, E. (1969). *Where the action is: Three essays*. Lane, Allen.

Grabosky P. (2015). *Cybercrime*. Oxford University Press.

Grabosky, PN., Smith, RG., and Dempsey, G.(2001). *Electronic theft: Unlawful acquisition in cyberspace*. Cambridge University Press.

Hauch, V., Blandón-Gitlin, I., Masip, J., and Sporer, SL. (2015). "Are computers effective lie detectors? A meta-analysis of linguistic cues to deception." *Personality and Social Psychology Review* 19(4): 307-342.

Herley, C. (2012). "Why do nigerian scammers say they are from nigeria?." In *WEIS*.

Ho, SM., Hancock, JT., Booth, C., Liu,X., Timmarajus, ST and Burmester, M. (2015). "Liar, Liar, IM on Fire: Deceptive language-action cues in spontaneous online communication." In *Intelligence and Security Informatics (ISI), 2015 IEEE International Conference on*, pp. 157-159.

Holt, TJ., and Graves, D. (2007). "A qualitative analysis of advance fee fraud email schemes." *The International Journal of Cyber Criminology* 1: 137-154.

Holtfreter, K., Van Slyke, S., and Blomberg, TG. (2005). "Sociolegal change in consumer fraud: From victim-offender interactions to global networks." *Crime, Law and Social Change* 44(3): 251-275.

Holtfreter, K., Reisig, MD., and Pratt, TC. (2008). "Low self-control, routine activities, and fraud victimization." *Criminology* 46(1): 189-220.

Horvitz, EJ., and Apacible, JT. (2009). "Use of a bulk-email filter within a system for classifying messages for urgency or importance." U.S. Patent 7,565,403.

Ingram, JR., and Hinduja, S. (2008). "Neutralizing music piracy: An empirical examination." *Deviant Behavior* 29(4): 334-366.

Internet Crime Complaint Center. (2014). 2014 Internet Crime Report. Available at: https://pdf.ic3.gov/2017_IC3Report.pdf

Jakobsson, M., and Leddy, W. (2016). "Could you fall for a scam? Spam filters are passe. What we need is software that unmasks fraudsters." *IEEE Spectrum* 53(5): 40-55.

Johnson, EJ., Hershey, J., Meszaros, J., and Kunreuther, H. (1993). "Framing, probability distortions, and insurance decisions." In *Making Decisions About Liability And Insurance*, pp. 35-51. Springer Netherlands.

Kalman, YM., and Gergle, D. (2014). "Letter repetitions in computer-mediated communication: A unique link between spoken and online language." *Computers in Human Behavior* 34: 187-193.

Kotlyar, I., and Ariely, D. (2013). "The effect of nonverbal cues on relationship formation." *Computers in Human Behavior* 29(3): 544-551.

Kshetri, N. (2010). "The economics of click fraud." *IEEE Security & Privacy* 8.3: 45-53.

Lea, SEG, Fischer, P., and Evans, KM. (2009)."The psychology of scams: Provoking and committing errors of judgement."

Long, SJ. (1997). "Regression models for categorical and limited dependent variables." *Advanced quantitative techniques in the social sciences*.

Long, SJ., and Freese, J. (2006). *Regression models for categorical dependent variables using Stata (2nd ed.)*. College Station, TX: Stata Press Publication.

Luckenbill, DF. (1977). Criminal homicide as a situated transaction. *Social problems*, *25*(2), 176-186.

Maruna, S. (2010). "Mixed method research in criminology: Why not go both ways?." In *Handbook of quantitative criminology*, pp. 123-140. Springer New York.

Meier, RF., Kennedy, LW., and Sacco, VF. (2001). "Crime and the criminal event perspective." *The process and structure of crime: Criminal events and crime analysis* 9: 1-28.

Muscanell, NL., Guadagno, RE., and Murphy, S. (2014). "Weapons of influence misused: A social influence analysis of why people fall prey to internet scams". *Social and Personality Psychology Compass* 8(7): 388-396.

Moustakas, E., Ranganathan, C., and Duquenoy, P. (2006). "E-mail marketing at the crossroads: A stakeholder analysis of unsolicited commercial e-mail (spam)." *Internet research* 16(1): 38-52.

Osgood, WD., Wilson, JK., O'malley, PM., Bachman, JG., and Johnston, LD. (1996). "Routine activities and individual deviant behavior." *American Sociological Review* : 635-655.

Osgood, WD. (2000). "Poisson-based regression analysis of aggregate crime rates." *Journal of quantitative criminology* 16(1): 21-43.

Pak, J., and Zhou, L. (2014). "Social structural behavior of deception in computer-mediated communication." *Decision Support Systems* 63: 95-103.

Park, Y., Jones, J., McCoy, D., Shi, E., and Jakobsson, M. (2014). "Scambaiter: Understanding targeted nigerian scams on craigslist." *system* 1: 2.

Petty, RE., and Cacioppo, JT. (1986). "The elaboration likelihood model of persuasion." In *Communication and persuasion*, pp. 1-24. Springer New York.

Pratt, TC., Holtfreter, K., and Reisig, MD. (2010). "Routine online activity and internet fraud targeting: Extending the generality of routine activity theory." *Journal of Research in Crime and Delinquency* 47(3): 267-296.

Reyns, BW., and Henson, B. (2016). "The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory." *International journal of offender therapy and comparative criminology* 60 (10): 1119-1139.

Roberds, W. (1998). "The impact of fraud on new methods of retail payment." *Economic Review-Federal Reserve Bank of Atlanta* 83(1): 42.

Shichor, D.,. Sechrest, DK., and Doocy, J. (2001). ‘‘Victims of Investment Fraud.’’ Pp. 81- 96. In Contemporary Issues in Crime and Criminal Justice, edited by H. N. Pontell and D. Shichor. Upper Saddle River, NJ: Prentice Hall Publishing.

Short, JF. (1998)."The level of explanation problem revisited—The American Society of Criminology 1997 presidential address." *Criminology* 36(1): 3-36.

Shover, N., Coffey, GS., and Hobbs, D. (2003)."Crime on the line. Telemarketing and the changing nature of professional crime." *British Journal of Criminology* 43(3): 489-505.

Tusan, C. (2014). Online sellers stung by scammers spoofing PayPal brand. available at : https://www.consumer.ftc.gov/blog/online-sellers-stung-scammers-spoofing-paypal-brand

Van Wilsem, J. (2013). "‘Bought it, but never got it’assessing risk factors for online consumer fraud victimization." *European Sociological Review* 29 (2); 168-178.

Wang, J., Herath, T., Chen, R., Vishwanath, A., and Rao, HR. (2012). "Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email." *IEEE Transactions on Professional Communication* 55(4): 345-362.

Welch, M., Fenwick, M., and Roberts, M. (1998). "State managers, intellectuals, and the media: A content analysis of ideology in experts' quotes in feature newspaper articles on crime." *Justice Quarterly* 15 (2): 219-241.

White, CH., and Burgoon, JK. (2011). "Adaptation and communicative design." *Human Communication Research* 27(1): 9-37.

Whitty, MT. (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.

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

Whitty, MT. (2015b). "Mass-marketing fraud: a growing concern." *IEEE Security & Privacy* 13(4): 84-87.

Wright, RT., and Decker, SH. (1994). *Burglars on the Job*. Boston, MA: Northeastern University Press.

Wright, RT., and Decker, SH.. (2011). *Armed robbers in action: Stickups and street culture*. UPNE.

Table 1. Descriptive Statistics (N=623 Email Threads)

Variable	Mean	Std. Dev.	Min-Max
Dependent Variables			
Subsequent Non-Verbal Cue of Urgency (# of emails)	2.59	2.35	0-15
Subsequent Verbal Cues of Urgency	0.70	0.45	0-1
Independent Variables			
Ad Content			
Auto part	0.12	0.49	0-1
Cellphone	0.24	0.42	0-1
Computers	0.28	0.45	0-1
Jewelry	0.36	0.48	0-1
Price ($)	138.80	158.40	11-700
Ad location			
Major metropolitan	0.45	0.50	0-1
Scammer's First Email Content			
Initial Verbal Cues of Urgency	0.18	0.38	0-1
Research Team Response			
Confirmation of target suitability	0.20	0.40	0-1

Table 2. Subsequent Verbal Cues of Urgency Regressed Over Ad Features and Scammers' Initial Correspondence with Targets (N=623 Email Threads)

Variables	Model 1		Model 2		Model 3	
	Coeff (SE)	Odds Ratio	Coeff (SE)	Odds Ratio	Coeff (SE)	Odds Ratio
Scammers' First Email Content						
Initial Verbal Cues of Urgency	.51+ (.30)	1.66	.10 (.35)	1.10	.17 (.36)	1.18
Research Team Response						
Confirmation of target suitability	-	-	-.18 (.21)	.83	-.10 (.21)	.90
Interaction						
Confirmation of target suitability × Initial Verbal Cues of Urgency	-	-	1.66* (.85)	5.29	1.60* (.85)	4.60
Ad Content [a]						
Cellphone	-	-	-	-	-.43 (.31)	.65
Computers	-	-	-	-	.13 (.33)	1.13
Jewelry	-	-	-	-	-.69 (.28)	.50
Price ($)	-	-	-	-	-.01 (.01)	.98
Ad Location						
Major metropolitan	-	-	-	-	-.02 (.17)	.98
Constant	.52*** (.09)		.56*** (.10)	-	1.07*** (.21)	-
Pseudo-R^2	.05		.05		.09	
AIC	817.3		816.45		804.70	
Log Likelihood	-406.65**		-404.25**		-397.36**	

[a] Reference category = auto parts

+p ≤ .10; *p ≤ .05; **p<0.01; ***p<0.001

Table 3. Subsequent Non-Verbal Cues of Urgency Regressed Over Ad Features and Scammers' Initial Correspondence with Targets (N=623 Email Threads)

Variables	Model 1		Model 2		Model 3	
	Coeff (SE)	Event Ratio	Coeff (SE)	Event Ratio	Coeff (SE)	Event Ratio
Scammers' First Email Content						
Initial Verbal Cues of Urgency	.27*	1.31	.06	1.06	.01	1.01
	(.11)		(.14)		(.14)	
Research Team Response						
Confirmation of target suitability	-	-	-.12	.89	-.18	.84
			(.09)		(.09)	
Interaction						
Confirmation of target suitability × Initial Verbal Cues of Urgency	-	-	.60**	1.83	.61**	1.85
			(.23)		(.23)	
Ad Content [a]						
Cellphone	-	-	-	-	.48***	1.61
					(.13)	
Computers	-	-	-	-	.29*	1.34
					(.14)	
Jewelry	-	-	-	-	.51***	1.66
					(.12)	
Price ($)	-	-	-	-	-.00	.99
					(.00)	
Ad Location						
Major metropolitan	-	-	-	-	-.18**	.83
					(.07)	
Constant	.80***		.82***	-	.53***	-
	(.04)		(.04)		(.11)	
Ln alpha	-1.19		-1.22		-1.33	
Pseudo-R^2	.04		.05		.11	
AIC	2455.90		2450.47		2438.60	
Log Likelihood	-1196.95**		-1193.63**		-1178.53**	

[a] Reference category = auto parts

+p ≤ .10; *p ≤ .05; **p<0.01; ***p<0.001

Figure 1. Predicted Probability of Verbal Cues of Urgency at Follow Up (N = 623 Email Threads)

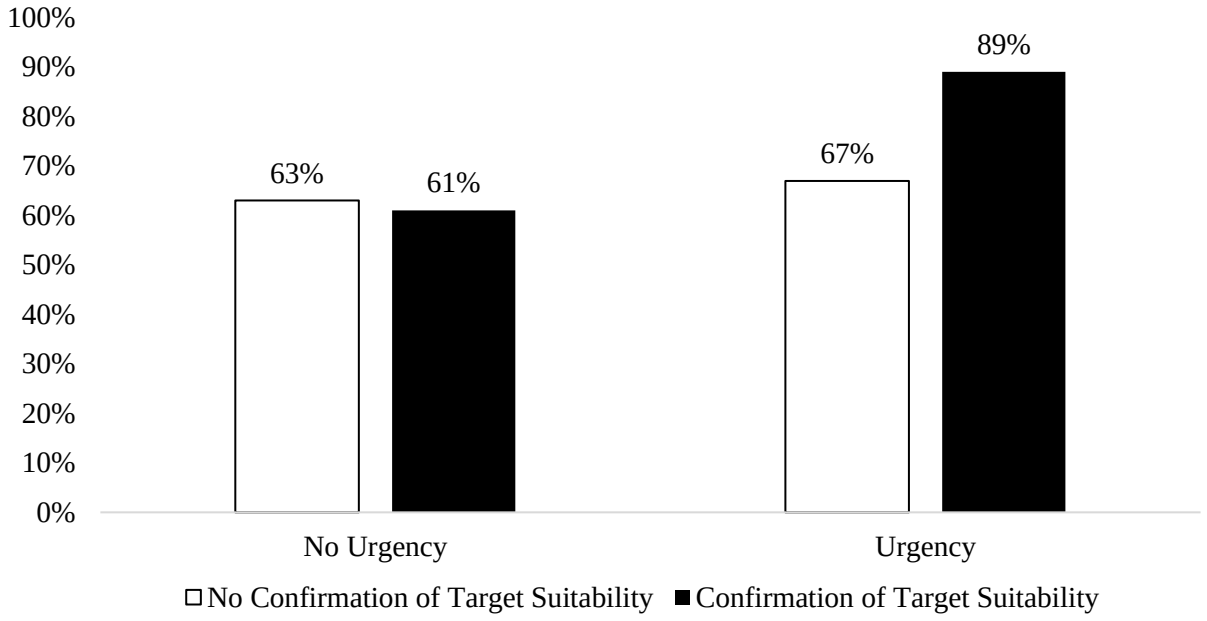
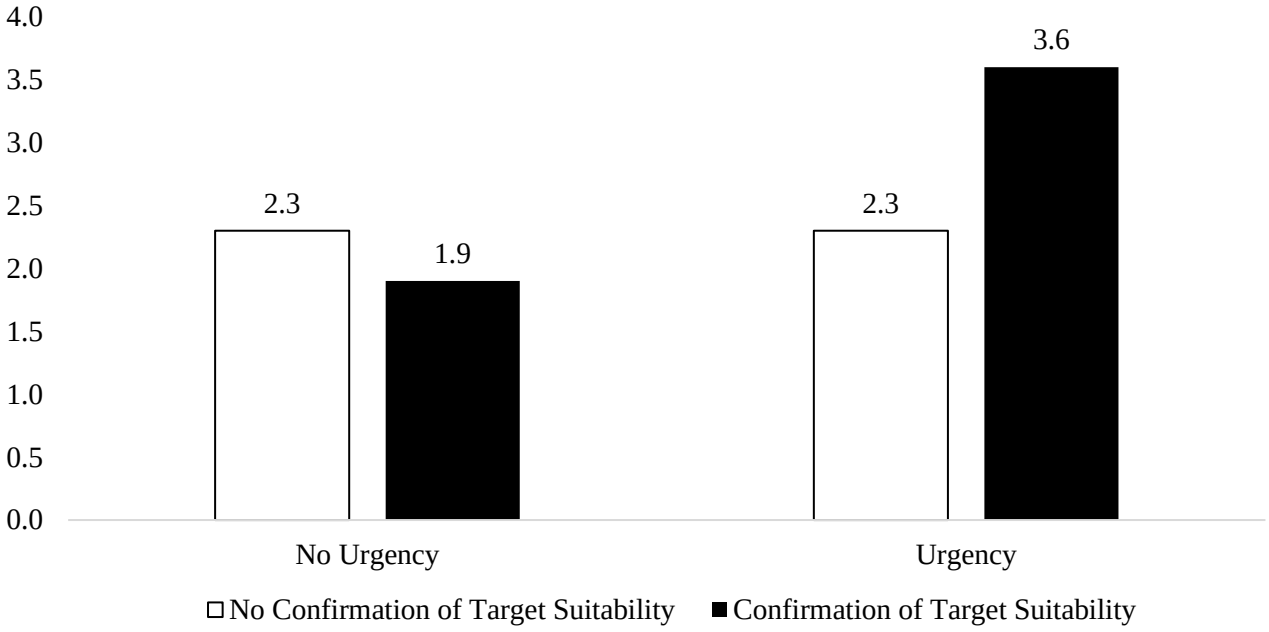


Figure 2. Predicted Number of Subsequent Email Responses (N = 623 Email Threads)



ENDNOTES

[1] The strategic behaviors and communication patterns that could be employed by deceivers include delivering false and ambiguous messages to their targets, creating distance between themselves and others, and presenting an image of a sincere and trustworthy individual.

[2] In order not to interfere with the regular ad traffic on the website, we made sure that our advertisements accounted for only a small fraction of the total ads volume in each of the cities.

[3] No significant differences were found between the type of products and locations of advertisement that were deleted by the website owner and those that were not.

[4] We adhered to the classified ad website's terms of use and restricted each of our accounts to posting in a single location, and at a posting rate of once every 48 hours.

[5] In analysis not shown, we restricted our sample to include email threads in which the content of the first email received in our email inboxes was significantly different across other first emails we received. Indeed, since the content of the first email we received from some of the potential costumers/online scammers was identical in 4% of the cases, one may suggest that those emails were sent from the same individuals. Re-estimating all the models reported in this manuscript while restricting the sample to email thread with "unique" first emails yielded consistent results to those reported in the manuscript.