4

Understanding Online Work-at-Home Scams through an Analysis of Electronic Mail and Websites

Sarah Turner, Heith Copes, Kent R. Kerley, and Gary Warner

Fraud has been a concern since the advent of modern economic systems. Historically, fraud involved direct interaction between victims and offenders, such as telephone-based communications or face-to-face interactions (Kitchens 1993; Knutson 1996; Stevenson 1998). The increase in the use of electronics for business and personal reasons has provided new opportunities for fraud (Grabosky, Smith, and Dempsey 2001; Wall 2001; Wire Fraud 2010). Offenders are now able to access a much larger number of victims faster and with fewer resources by using the Internet than by using previous mediums (Savona and Migone 2004). This growth in opportunities is likely responsible for the rise in fraud over the past decade (Shover and Hochstetler 2006; Symantec 2010).

The reliance on email for communication in recent decades has made it an ideal place to search for targets. Fraudsters have increasingly turned to spam email messages to facilitate their illegal behaviors. By using this approach, offenders are able to send massive amounts of unwanted emails with little or no direct costs. For example, large-scale distribution of spam messages, referred to as "spam campaigns," may include millions of emails sent around the world in only a few hours. Some estimate that spammers send 130.5 billion email messages each year, which accounts for 89.1% of all email sent (Symantec 2010).

Many spam campaigns have a clear intent to defraud individuals of their money, property, or personal information (Yu 2011). There are multiple types and uses of spam, most of which are responsible for financial damages (i.e., pharmaceutical spam or phishing emails). However, many of these types of spam emails have not been studied widely, especially from a social science perspec-

tive. Here we focus on "work-at-home" spam as an emerging form of online fraud. This fraud solicits participation in a variety of scams that promise "big money" for just a few hours of work per day, all of which can be done at home. In one recent example of this type of fraud, Google sued Pacific WebWorks for trademark infringement, dilution, unfair competition, and federal cyber piracy (ABC News 2009). The 2009 suit alleged that Pacific WebWorks victimized consumers by prominently displaying the Google logo, by suggesting sponsorship by Google, and by urging consumers to obtain a kit designed to help them work at home with Google products. According to Google officials, thousands of individuals had been tricked into sending payment information and then were charged for hidden fees and renewable subscriptions. The average loss per consumer was just under $100 (ABC News 2009).

Despite being responsible for significant financial losses, relatively little is known about online work-at-home fraud. Given the relative anonymity of the offenders and the significant monetary damages associated with this fraud, our goal in this exploratory study is to identify the common characteristics of a representative sample of work-at-home spam derived from a proprietary database. In doing so we shed light on trends in this type of fraud, techniques fraudsters use to enhance the legitimacy of the proposition, and elements of the solicitations that may be attractive to potential victims.

Work-at-Home Scams

A work-at-home scam is a fraudulent opportunity where the goal is to extort money from victims by luring them with offers to be employed at home. Typically the offer involves performing simple tasks for a short amount of time each day while earning an amount that far exceeds market value. These scams encompass many work-at-home opportunities, such as secret shoppers, stuffing envelopes, multi-level marketing (i.e., pyramid schemes), product sales, processing medical or insurance claims, or repackaging and shipping.

One example is a "secret shopper" scam in which potential employees are required to pay upfront fees that will cover training materials and/ or membership to a database of secret shoppers from which corporations can hire. The secret shopper scheme usually is advertised as not requiring any previous experience, special training, or advanced education. In these scams fraudsters prey on victims by advertising the ability to earn money simply by shopping. The "employees" are provided a check or money order to purchase merchandise at specific retailers and, on average, are offered 10% of each check or money order as compensation. After purchasing the requested items with the provided funds and

writing a report on their shopping experience, the s
chased items to a designated location and send the
transfer (ABC News 2008). This type of secret sho
porates elements of a "re-shipping scam" and a "c
scams are used to launder money or goods, as well
ing victims cash potentially fraudulent checks. In
victims may suffer identity theft and face criminal c
of work being performed (Internet Crime Compla
As with any emerging fraud, reliable data on the
economic impact of work-at-home scams is not re
data contributes to a lack of knowledge (for both
about the crime, which makes developing effective
is a substantial "dark figure" associated with any type
mann 1995), preliminary data on work-at-home fr
intelligence reports of many major companies. Acc
work-at-home spam is now ranked as the fifth mos
is estimated as being responsible for 4,306,500,000
ing the year 2010. Results from the 2010 Symante
used to estimate the impact of work-at-home spar
sages and typical startup fee of $19.95 or greater.
(430,640) of individuals who received a work-at-h
time startup fee of $19.95, it would create over $8.

Online Fraud in Co

While there is a lack of information about the
at-home spam, there are several recent studies o
many of which involve spam email. Yu (2011) st
ternet spam messages to determine their conte
compliance with the Federal Trade Commission'
researcher gathered 3,983 spam messages from
for a four-month period during 2010. Nearly h
written in HTML, over one-third used images,
in English. Interestingly, of the nearly 4,000 mes
a clear violation of the CAN-SPAM Act. Nhan,
studied spam email via an analysis of two email
time period. During the months in which the accou
emails were received and identified as potentiall
then categorized the messages along a broad ra

writing a report on their shopping experience, the shoppers then ship the purchased items to a designated location and send the remaining money by wire transfer (ABC News 2008). This type of secret shopping arrangement incorporates elements of a "re-shipping scam" and a "cashier's check scam." Both scams are used to launder money or goods, as well as to extort money by having victims cash potentially fraudulent checks. In addition to financial losses, victims may suffer identity theft and face criminal charges based upon the type of work being performed (Internet Crime Complaint Center 2010).

As with any emerging fraud, reliable data on the incidence, prevalence, and economic impact of work-at-home scams is not readily available. This lack of data contributes to a lack of knowledge (for both the legislature and public) about the crime, which makes developing effective policy difficult. While there is a substantial "dark figure" associated with any type of fraud (Titus and Heinzelmann 1995), preliminary data on work-at-home fraud can be gleaned from the intelligence reports of many major companies. According to Symantec (2010), work-at-home spam is now ranked as the fifth most prevalent type of spam and is estimated as being responsible for 4,306,500,000 (3.3%) spam messages during the year 2010. Results from the 2010 Symantec Intelligence Report can be used to estimate the impact of work-at-home spam using the number of messages and typical startup fee of $19.95 or greater. Thus, if only 1/1000 of 1% (430,640) of individuals who received a work-at-home spam email paid a one-time startup fee of $19.95, it would create over $8.5 million in monetary losses.

Online Fraud in Context

While there is a lack of information about the nature and content of work-at-home spam, there are several recent studies of fraudulent online schemes, many of which involve spam email. Yu (2011) studied the broad topic of Internet spam messages to determine their content, format, techniques, and compliance with the Federal Trade Commission's 2004 CAN-SPAM Act. The researcher gathered 3,983 spam messages from five separate Gmail accounts for a four-month period during 2010. Nearly half of all the messages were written in HTML, over one-third used images, and nearly 60% were written in English. Interestingly, of the nearly 4,000 messages, only 108 did not have a clear violation of the CAN-SPAM Act. Nhan, Kinkade, and Burns (2009) studied spam email via an analysis of two email accounts over a three-month time period. During the months in which the accounts were active, 476 unsolicited emails were received and identified as potentially fraudulent. The researchers then categorized the messages along a broad range of variables such as busi-

nesses or industries mentioned, profession of sender, personal information provided by sender, nature of the message, amount of money involved, amount of return expected on investment, and the target information requested. Overall, they found that fraudsters tended to prefer a "social engineering" method of obtaining victims' personal and financial information, as opposed to more direct inquiry about sensitive information.

Edelson (2003) studied the 419 Nigerian advance fee fraud scam to identify key characteristics of those emails. The 419 scam is a unique form of fraud that is perpetrated through letters, fax, email, and websites. These scams are a concern not only for the estimated five billion dollars lost worldwide during the 1990s, but also for the enormous volume of spam fraudsters send and the associated security risks. Analyzing the headers of 1,000 emails, Edelson found that the 419 emails operated primarily, but not exclusively, from West Africa and Europe. Emails typically contained multiple methods of communication (i.e., telephone numbers, fax numbers, pagers, and emails) and the content often ended in the middle of a paragraph. To combat the concerns associated with this spam, Edelson recommends that email providers employ better filtering methods to prevent the emails from being sent.

Holt and Graves (2007) focused on other types of advance fee fraud. They conducted a qualitative analysis of 412 advance fee fraud emails received in two separate inboxes over two years. The purpose of Holt and Graves' study was to analyze the message syntax and to identify any traits or patterns that increased the likelihood of victimization. The authors compared multiple aspects of the email structure and content to identify both common and unique characteristics so they could better identify advance fee fraud emails. The findings suggest that 419 scammers attempt to include data that can increase impressions of legitimacy by employing unique phrasing throughout each email, enticing subject lines, or appeal to victims by mentioning potential monetary earnings. Their findings were used to improve knowledge of Internet fraud and identity theft by the general public as well as by law enforcement agencies. In addition to encouraging Internet service providers to employ better filtering methods, the authors advocate public awareness programs and more empirical research to identify any similarities between victims as a possible means of understanding the enticements.

Hu, McInish, and Zeng (2010) investigated how spam emails that promoted stock tips might influence the decision-making processes of active stock traders. The researchers gathered over 40,000 spam messages touting 785 firms in 580 spam campaigns over a nearly three-year period. The five key aspects of the spam messages analyzed were target price of the stock, message length, email source, incentives for purchase, and whether the businesses touted were international. Of these five aspects, Hu et al. (2010) found that target price and international businesses were the two most important aspects. Specific was most likely to be impacted by the spam campaigns wher of the stock was mentioned and when the businesses toute Rege (2009) added to the literature by examining fraudulen from 2000 to 2009. Specifically, the researcher identified 17 from dating sites, news and media sites, anti-scam commi ment agencies, and government agencies for analysis. The velop a typology of cyber offenders involved in online d includes their techniques, motivation, and organization.

In this paper we build on these previous studies to ex fraud. That is, we explore trends in this type of fraud, tech sters, and elements of the solicitations that may be attrac tims. We analyze a representative sample of work-at-hom corresponding websites derived from a proprietary databa panding the limited amount of research on work-at-hon study will identify key characteristics of work-at-home er

Data and Methodology

This pilot study examines work-at-home emails and th links derived from the University of Alabama at Birmingh The Spam Data Mine receives over 1.5 million messages have been used for research in spam, phishing, and ma Warner 2008; Wei, Sprague, and Warner 2009; Wei, Spra lum 2010). We began our study in January, 2011, by foc recent months of data from the Spam Data Mine. Because a large collection of emails, Structured Query Language row the results based on the subject lines of the emails a they were sent. Subject lines such as "work from home," home," and "extra cash" were used in the queries to r work-at-home emails. This database query yielded 8,01 2010, and 7,200 emails for December 2010. The results returned a subject line and unique identifier[1] for each sentative sample of emails from each month with a 9 and a 10% sampling error. Given that each month ha

1. The unique identifier is a tag assigned to every email rec is to expedite queries and allow better organization within the the date received as well as the time, an example is iid.10Nov(

businesses were the two most important aspects. Specifically, stock trading was most likely to be impacted by the spam campaigns when a short-term price of the stock was mentioned and when the businesses touted were U.S.-based. Rege (2009) added to the literature by examining fraudulent online dating sites from 2000 to 2009. Specifically, the researcher identified 170 online documents from dating sites, news and media sites, anti-scam commissions, law enforcement agencies, and government agencies for analysis. The purpose was to develop a typology of cyber offenders involved in online dating scams, which includes their techniques, motivation, and organization.

In this paper we build on these previous studies to explore work-at-home fraud. That is, we explore trends in this type of fraud, techniques of the fraudsters, and elements of the solicitations that may be attractive to potential victims. We analyze a representative sample of work-at-home spam messages and corresponding websites derived from a proprietary database. In addition to expanding the limited amount of research on work-at-home spam, the present study will identify key characteristics of work-at-home emails and websites.

Data and Methodology

This pilot study examines work-at-home emails and their embedded website links derived from the University of Alabama at Birmingham's Spam Data Mine. The Spam Data Mine receives over 1.5 million messages daily and its resources have been used for research in spam, phishing, and malware (Wardman and Warner 2008; Wei, Sprague, and Warner 2009; Wei, Sprague, Warner, and Skjellum 2010). We began our study in January, 2011, by focusing on the two most recent months of data from the Spam Data Mine. Because the data mine has such a large collection of emails, Structured Query Language (SQL) was used to narrow the results based on the subject lines of the emails and the month in which they were sent. Subject lines such as "work from home," "job available," "stay at home," and "extra cash" were used in the queries to return a relevant list of work-at-home emails. This database query yielded 8,014 emails for November 2010, and 7,200 emails for December 2010. The results from the subject query returned a subject line and unique identifier[1] for each email. We drew a representative sample of emails from each month with a 95% confidence interval and a 10% sampling error. Given that each month had a population between

1. The unique identifier is a tag assigned to every email received in the data mine. This is to expedite queries and allow better organization within the database. Each tag includes the date received as well as the time, an example is iid.10Nov01.1111.

5,000 and 10,000, we needed to select at least 95 emails from each month to achieve a representative sample (Salant and Dillman 1994). We then oversampled slightly to reach 100 emails per month, for a total sample of 200.

Each selected identifier number was used to find the body of the email in the Data Mine. Once the corresponding emails were located, the content was checked to ensure it advertised for a work-at-home opportunity. Emails were considered fitting sampling criteria if they contained content relating to any form of a work-at-home opportunity. If so, the emails were exported, the subject recorded for analysis, the website links included in the message content were documented, and the corresponding email was tagged as having contained an active link.

Any website address appearing in the body of the email was then selected as a second source of data. Documented website addresses were pasted into an Internet browser to capture screenshots and Whois information for the work-at-home sites.[2] The website links were followed as quickly as possible because these sites have a high rate of change. This is due, in part, to "black lists" (i.e., lists of websites deemed scams or potential threats that are not only available to the public but also are sent to email and Internet service providers), email recipients alerting their email providers of potential scam emails, and Internet Service Providers blocking or shutting down suspected scam sites. Using this method we identified a total of 59 websites embedded in the 200 emails.

We determined that the best methodological approach for this data was content analysis, and thus developed separate coding sheets for the emails and the websites. While similar in coding content, the nature of the formats dictated that we code them differently. Whereas the emails were better suited for textual analysis, the websites also contained numerous images that could be analyzed. For the emails, we sought information about the financial details mentioned, claims of legitimacy, use of personalization or flattery, and locations from which the emails were sent. When coding for legitimacy we looked for characteristics such as whether the sender provided a physical address or other contact information, whether they mentioned well-known legitimate companies, and whether they mentioned other solicitations that could be scams. When coding for personalization we focused on mentions of the sender's or recipient's gender, mentions of the recipients' names, or the use of flattery (e.g., describing the recipients as "smart" or as "good business people").

When coding the websites we sought to determine the overall format of the websites. The websites came in one of six variations: news website, piggyback

2. Whois.domaintools.com is a free website that offers information about an IP address or website such as website registrar, name server, contact information for the domain owner, create/expiration/update dates for websites, and much more.

on legitimate cites, a "regular" website advertising work at
ing a service/item to assist in your work at home success,
the visitor to either input personal data or request inform
uct/service being described, or other/unknown. There w
als in websites than in email so we coded for the number
the gender of those giving them. When coding for the financ
sites we included dollar amounts that appeared in the tex
peared in images (e.g., photos of checks). Finally, we code
of legitimacy. These included whether well-known legitin
mentioned and if so, how many, if other scams were me
cation on the website where these mentions were found.

Once coding for email and message content was com
about the legitimacy of the email and websites was collecte
each website address was collected using Whois.domain
and the UAB Geolocator. This information included scr
dress of the domain, the domain name, Whois data, the
the actual geographic region to which the IP address belc
included the location of the IP address owner, when the
when it expires, and the ICANN registrar (i.e., the person
was registered and the person responsible for the webs
mation on the legitimacy of the email we reviewed the h
establish if the email had been "spoofed" (faked or forg
main), where the IP originated from, and any discrepanci
email address and the "reply to" address.

Identifying the originating IP and header informati
with the same steps. Some email clients provide the s
"Originating IP" inside the email header, but other ema
is in those instances that the IP can be found by workin
parent originating IP by comparing the "received from"
ing that the supplied IP addresses resolve to the reporte
did not match then the header had most likely been spoo
the email service providers for the recipients of the sc
that the header had been spoofed and/or was part of a sp
was any uncertainty while manually classifying a header,
or the online application IP Address Location were use

3. Compete is a monthly ranking system that counts unique vi
sites with the most visitors have higher ranks.

4. Because of how the emails are stored in the data mine, it
the full header of every email.

on legitimate cites, a "regular" website advertising work at home offers, offering a service/item to assist in your work at home success, a website requiring the visitor to either input personal data or request information on the product/service being described, or other/unknown. There were more testimonials in websites than in email so we coded for the number of testimonials and the gender of those giving them. When coding for the financial details from websites we included dollar amounts that appeared in the text and those that appeared in images (e.g., photos of checks). Finally, we coded websites for claims of legitimacy. These included whether well-known legitimate companies were mentioned and if so, how many, if other scams were mentioned, and the location on the website where these mentions were found.

Once coding for email and message content was completed, information about the legitimacy of the email and websites was collected. Information about each website address was collected using Whois.domaintools.com, FlagFox, and the UAB Geolocator. This information included screen shots, the IP address of the domain, the domain name, Whois data, the Compete rank,[3] and the actual geographic region to which the IP address belongs. The Whois data included the location of the IP address owner, when the website was created, when it expires, and the ICANN registrar (i.e., the person to whom the domain was registered and the person responsible for the website). To collect information on the legitimacy of the email we reviewed the header of the email to establish if the email had been "spoofed" (faked or forged IP address or domain), where the IP originated from, and any discrepancies between the "from" email address and the "reply to" address.

Identifying the originating IP and header information was accomplished with the same steps. Some email clients provide the sender's IP address as "Originating IP" inside the email header, but other email providers do not. It is in those instances that the IP can be found by working backwards to the apparent originating IP by comparing the "received from" lines and then verifying that the supplied IP addresses resolve to the reported domains. If the lines did not match then the header had most likely been spoofed. In some instances, the email service providers for the recipients of the scam emails recognized that the header had been spoofed and/or was part of a spam campaign. If there was any uncertainty while manually classifying a header, the tools Ping, Whois, or the online application IP Address Location were used for verification.[4]

3. Compete is a monthly ranking system that counts unique visitors of websites. The websites with the most visitors have higher ranks.

4. Because of how the emails are stored in the data mine, it was not possible to retrieve the full header of every email.

Once the originating IP and domain were identified (if possible), that information was then compared to the "from" tag to again check for any attempts at spoofing. The "from" tag was then compared to the "reply to" tag to check for consistency. This comparison was necessary because if the "from" address was spoofed to look like it came from a well-known company or group, the scammer would need to have a different "reply to" email address to access any replies received from that email.

Analysis of Emails

Table 1 provides a summary of the content of the email messages. The first element recorded for the emails was whether the message was comprised of text and no link, a link and no text, or both a text and a link. The majority of the emails (77%) contained both text and a link in the message body, 20% consisting of text only, and 3% consisted of links only. The emails with text offered more details of the scam being promoted than emails with links. Although a large percentage of the website links were not active, we note that 74% of the emails requested a response via a website. Approximately 28% of the emails used HTML graphics and nearly 90% used a "testimonial" about the work opportunity. The median length of email message was 151 words.

In Table 2 we describe the extent to which the emails were personalized and targeted to potential victims. As shown in Table 2, we found that 49% of the messages did not include any reference to the gender of the email sender (i.e., they were not signed or used the advertised company or group name in closing). Those that included the gender of the sender were almost twice as likely to be male than female. In situations where the gender was identified, it was typically through the introduction of the email, and in most instances (77.5%) there was no mention of any professional credentials of the sender (i.e., no formal closing or mention of a job title or position). The majority (90.5%) of emails did not contain a gender-specific greeting, whether it was a name or other, such as "Hey Daniel," or "good morning ma'am." When gender was mentioned it was equally split.

In some circumstances, scammers personalized the email, either by including the recipient's email address in the message, the recipient's name,[5] or by using a less formal, friendlier writing style, such as, "Hey, I know money's

5. In most instances it was not possible to know if the included name was that of the recipient or a randomly generated one; however, if a name was present, it was coded as having been personalized.

Table 1. Message Content c

Message consists of	
Text only	
Link only	
Text and Link	
Response Method	
Website	
Email	
HTML Graphics	
Yes	
No	
Testimonial	
Yes	
No	
Message Length (words)	
Range	
Median	
Average	
Mode	

been tight and you've been busy work to hang out anymore."[6] While theor crease the probability of a response, message.

We also sought to determine the entice recipients. Flattery such as "o

6. This example, as well as others we sample.

Table 1. Message Content of Work-at-Home Email

	Frequency	Percent
Message consists of		
Text only	40	20.0
Link only	6	3.0
Text and Link	154	77.0
Response Method		
Website	148	74.0
Email	52	26.0
HTML Graphics		
Yes	55	27.5
No	145	72.5
Testimonial		
Yes	177	88.5
No	23	11.5
Message Length (words)		
Range	0–1113	
Median	151	
Average	98.65	
Mode	105	

been tight and you've been busy working which sucks since you never have time to hang out anymore."[6] While theoretically a more personal greeting may increase the probability of a response, 82.5% of senders did not personalize the message.

We also sought to determine the extent to which senders used flattery to entice recipients. Flattery such as "only intelligent individuals were given this

6. This example, as well as others we present throughout, is drawn from emails in our sample.

Table 2. Personalization and Targeting of Work-at-Home Email Content

	Frequency	Percent
Sender Gender		
Male	65	32.5
Female	37	18.5
Unknown	98	49.0
Recipient Gender		
Male	10	5.0
Female	9	4.5
Unknown	181	90.5
Greeting Personalization		
Yes	35	17.5
No	165	82.5
Flattery		
Yes	49	24.5
No	151	75.5

opportunity," can make the recipient feel emotionally linked to the sender and could increase the likelihood of response. For example, the scammer may give the impression that this work-at-home opportunity is only available to the "upper echelons of society" or to "intelligent members of society." Approximately 25% of the emails contained this writing style. This component of work-at-home scam emails is an example of other tools offenders may use to convince people to try a program.

We also examined several elements of the legitimacy of the message. Harley and Lee (2009, 5) have noted the importance of "brand association" in online scams because "it is considered an effective technique that allows scammers to directly steal information or be able to use social engineering to persuade users to disclose financial information." As shown in Table 3, 32% of the emails included the mention of a major company. Also, the same amount (32%) of emails mentioned the program's legitimacy. Two examples of legitimacy claims were:

Table 3. Message Legitimacy Claims i

	F
Scammer mentions a legitimate company	
Yes	
No	
Scammer mentions other scam/legitimacy of this program	
Yes	
No	
Mailing address included	
Yes	
No	
Personal sender information listed	
Yes	
No	
Grammar and spelling errors	
Yes	
No	

"I want to tell you about a REAL job
are—for well-known, legitimate con
and really need people who are willir
"What's more, I'd like you to know th
or schemes. No way. In fact, more
make a fulltime … or part-time …
raved about in the media. For examp
way to make extra cash.'"

Such claims demonstrate methods the s
victims and to put wary victims at ease.

Another aspect of legitimacy coded v
or sender information. The presence o

-HOME SCAMS

geting of
ent

Percent
32.5
18.5
49.0
5.0
4.5
90.5
17.5
82.5
24.5
75.5

linked to the sender and
e, the scammer may give
r is only available to the
ers of society." Approxi-
yle. This component of
ols offenders may use to

y of the message. Harley
sociation" in online scams
ows scammers to directly
to persuade users to dis-
f the emails included the
t (32%) of emails men-
imacy claims were:

Table 3. Message Legitimacy Claims in Work-at-Home Email

	Frequency	Percent
Scammer mentions a legitimate company		
Yes	64	32.0
No	136	68.0
Scammer mentions other scam/legitimacy of this program		
Yes	64	32.0
No	136	68.0
Mailing address included		
Yes	108	54.0
No	92	46.0
Personal sender information listed		
Yes	45	22.5
No	155	77.5
Grammar and spelling errors		
Yes	77	38.5
No	123	61.5

> "I want to tell you about a REAL job you can do from anywhere you are—for well-known, legitimate companies who pay well, pay fast, and really need people who are willing to be reliable for them."
> "What's more, I'd like you to know that this is not one of those scams or schemes. No way. In fact, more than 630,239 U.S. citizens now make a fulltime ... or part-time ... income this way. Plus, it's been raved about in the media. For example ... CNN News says it's, 'A great way to make extra cash.'"

Such claims demonstrate methods the scammers may use to entice potential victims and to put wary victims at ease.

Another aspect of legitimacy coded was the presence of a physical address or sender information. The presence of a physical address would imply that