FALSE CLAIMS IN SPAM

A report by the FTC's Division of Marketing Practices

April 30, 2003

FALSE CLAIMS IN SPAM

I. OVERVIEW

In this report, staff of the Federal Trade Commission's ("FTC") Division of Marketing Practices describes the results of its review of approximately 1,000 pieces of unsolicited commercial email (UCE), commonly known as "spam." This random sample was drawn from a pool of over 11,000,000 pieces of spam. This study, which focuses on the likely truth or falsity of claims contained in the messages, supplements two previous FTC studies of spam – the "Spam Harvest" (finding that 86% of addresses posted to web pages and newsgroups received spam) and the "Remove Me Surf" (finding that 63% of email list removal requests were not honored).

About 1,000 pieces of spam were analyzed to determine whether they bore the hall-marks of falsity.

This study represents the first extensive review of false claims appearing in UCE.[1] FTC staff who are trained to spot deceptive and unfair practices identified indicators of falsity for several types of offers likely to appear in spam. These indicators of falsity were based on representations found to be false in previous law enforcement actions brought by the Commission and on staff research. Staff then analyzed each piece of spam to determine whether the "From" line, "Subject" line, or message content contained any of these signs of falsity. The presence of signs of falsity in a message reviewed in this study does not mean that the message satisfies the legal standard of deception under the FTC Act; further investigation would be necessary to make such a determination. Staff also reviewed each piece of spam to determine whether the message contained pornographic images (in order to determine whether the nature of the images was disclosed in the "Subject" line), a request for personal information, or a label indicating that the message was an advertisement.

FTC staff analyzed false claims appearing in "From" and "Subject" lines and in the body of messages.

The messages reviewed by FTC staff consist of random samples from three FTC data sets – the UCE Database (consisting of spam forwarded to the FTC by members of the public), the Harvest Database (consisting of messages received by undercover FTC email boxes seeded on Internet web pages and in chat rooms), and spam received by FTC employees in their official FTC inboxes. A full description of the data sets, the sampling ratios, and likely biases of each data set are discussed in Section XI. (Methodology).

---

[1] Studies by others have focused on the economic costs resulting from spam (*see, e.g.*, (April 8, 2003)), the volume of UCE (Dec. 23, 2002)), and consumer attitudes regarding spam (*see, e.g.*, (Jan. 3, 2003)).

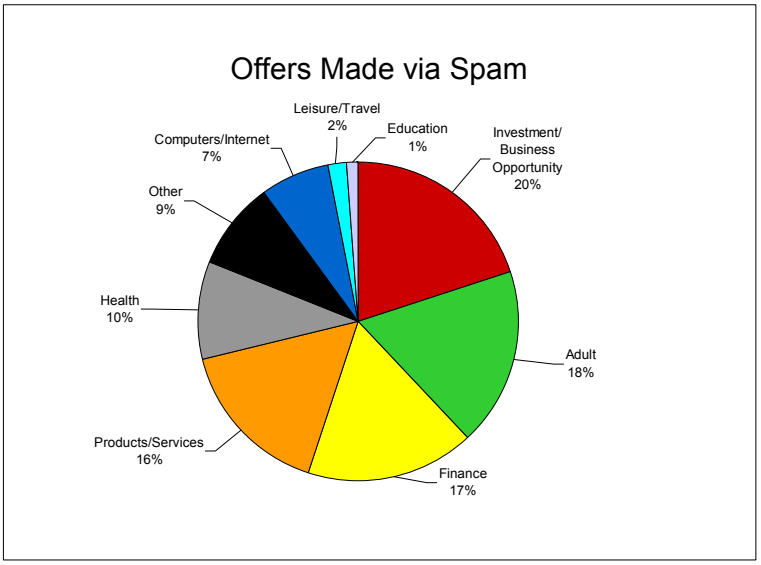
II. TYPES OF OFFERS MADE VIA SPAM

FTC staff began its analysis by determining the type of offer being made in each spam message. The messages fell into eight general categories, with a catch-all category included for types of offers that appeared infrequently:

Type of Offer	Description
Investment/Business Opportunity	work-at-home, franchise, chain letters, etc.
Adult	pornography, dating services, etc.
Finance	credit cards, refinancing, insurance, foreign money offers, etc.
Products/Services	products and services, other than those coded with greater specificity.
Health	dietary supplements, disease prevention, organ enlargement, etc.
Computers/Internet	web hosting, domain name registration, email marketing, etc.
Leisure/Travel	vacation properties, etc.
Education	diplomas, job training, etc.
Other	catch-all for types of offers not captured by specific categories listed above.

Investment/ Business Opportunity offers account for 20% of spam studied. The majority of these are work-at-home, franchise, chain letter, and other non-securities offers.

The following illustration sets forth the prevalence of different types of offers in the random sample of spam analyzed by FTC staff:



Investment/ Business Opportunity, Adult, and Finance offers together comprise over half of spam in sample.

Together, Investment/Business Opportunity, Adult, and Finance offers comprised 55% of the random sample of spam analyzed by FTC staff. Surprisingly, given that UCE inherently targets consumers with computers and Internet connections, only 7% of the spam analyzed concerned offers for computer or Internet-related products or services.

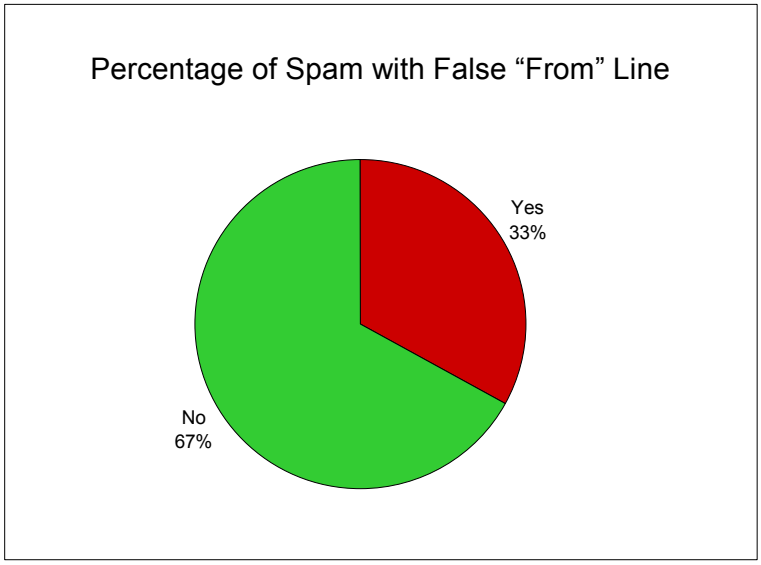
Only 7% of spam analyzed concerned Computer or Internet-related goods or services.

III. FALSITY IN "FROM" LINE

The "From" line in each UCE message was examined to determine whether the information obscured the true identity of the sender. FTC staff determined whether the "From" line contained any of the following indicators of falsity:

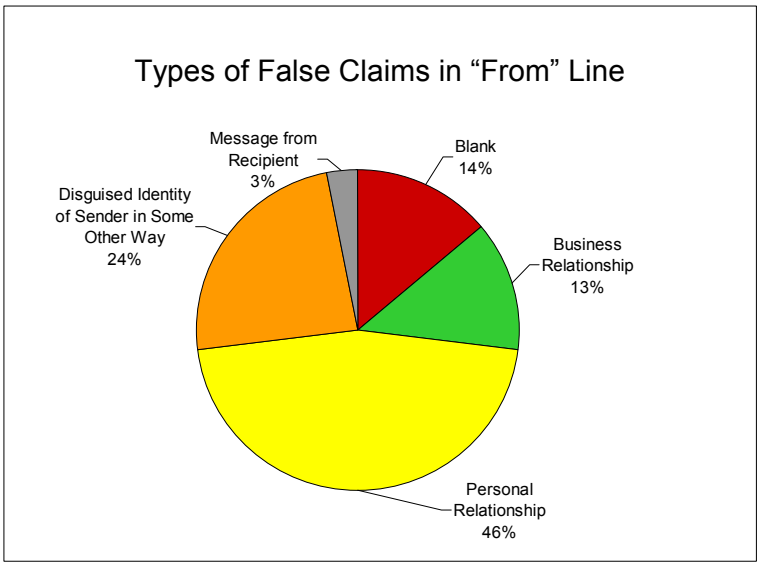
Type of "From" Line Falsity	Description
Blank	Sender's identity has been stripped from "From" line
Connotes Business Relationship	Name of sender suggests a business relationship between sender and recipient (e.g., "youraccount@vendorxyz.com")
Connotes Personal Relationship	Name of sender suggests a personal relationship between sender and recipient (e.g., use of first name only, which may suggest that the message is from someone in the recipient's address book.)
Message from Recipient	Sender's identifying information has been stripped from message and replaced with recipient's email address
Disguised in Other Way	Catch-all for other methods used to disguise the sender's true email address (e.g., sender, as identified in the message text, uses another person or entity's name or email address in the from line)

One-third of the spam messages contained false information in the "From" line.



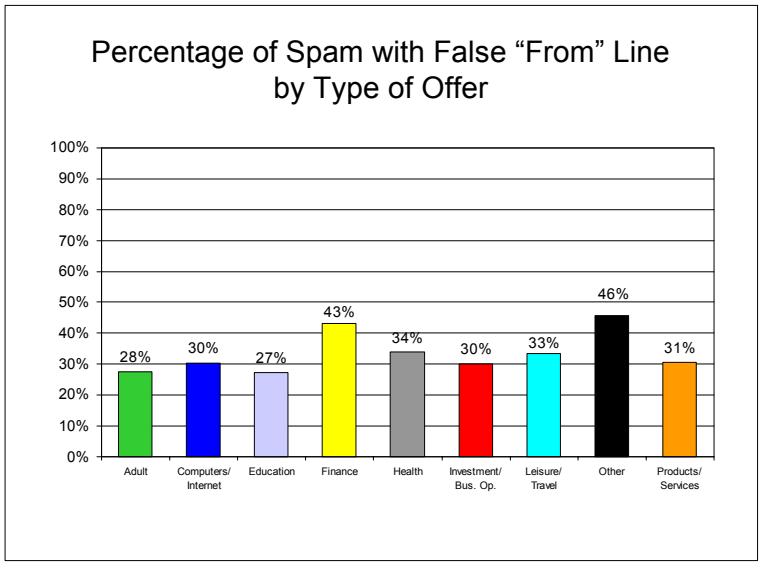
Thirty-three percent of spam analyzed contained false information in the "From" line.

Of the messages containing indicators of falsity in the "From" line, nearly half claimed to be from someone with a personal relationship with the recipient. Such a personal relationship was typically manifested by the use of only a first name in the "From" line, suggesting that the message was coming from someone whose name was in the recipient's email address book.



Of the spam containing false information in the "From" line, 46% suggested a personal relationship between the sender and recipient.

"From" lines with signs of falsity appeared in UCE for all types of offers, with incidence rates ranging from a low of 27.2% for education-related spam to a high of 45.8% for spam coded as "Other," and 43.1% for finance-related spam. No matter the type of offer contained in the UCE, senders of the UCE reviewed by FTC staff frequently obscured their identity by manipulating the information in the "From" line.



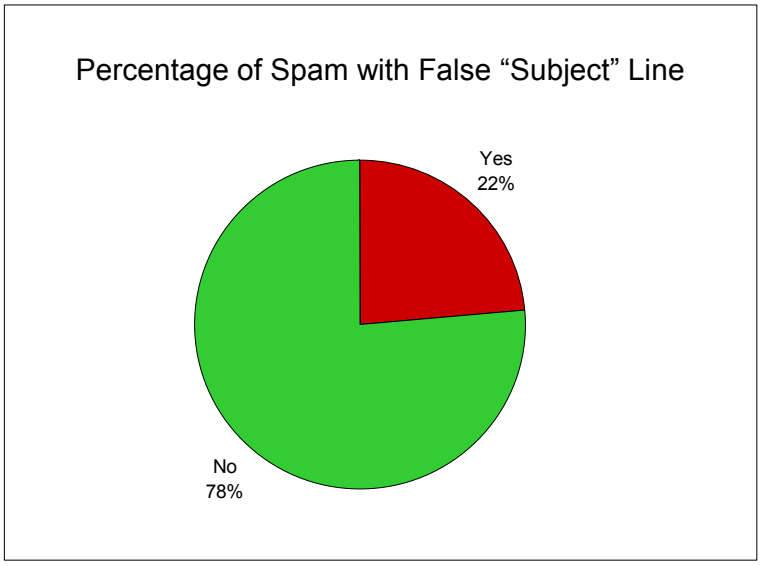
Senders of all types of spam analyzed frequently obscure their identities in the "From" line.

IV. FALSITY IN "SUBJECT" LINE

FTC staff examined the "Subject" line in each spam message in the sample to determine whether the information appeared to be false. "Subject" lines were analyzed to determine whether they contained any of the following characteristics:

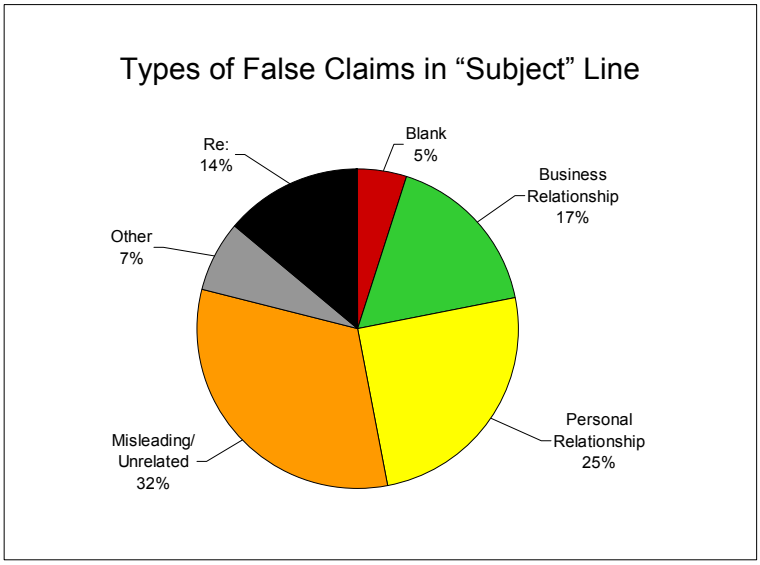
Type of Subject Line Falsity	Description
Blank	Contains no information about the subject of the message
Connotes Business Relationship	Suggests existence of business relationship between sender and recipient (e.g., "your order's status")
Connotes Personal Relationship	Suggests existence of personal relationship between sender and recipient (e.g., "Bob says 'hi'")
Unrelated to Content of Message	Content of message differs from description in "Subject" line
Re:	Suggests that the message is in reply to a message previously sent by recipient
Other	Catch-all for other methods used to disguise the true content of the message (e.g., "Subject" line indicates that the message is "extremely urgent.")

Twenty-two percent of UCE in the sample contained false information in the "Subject" line.



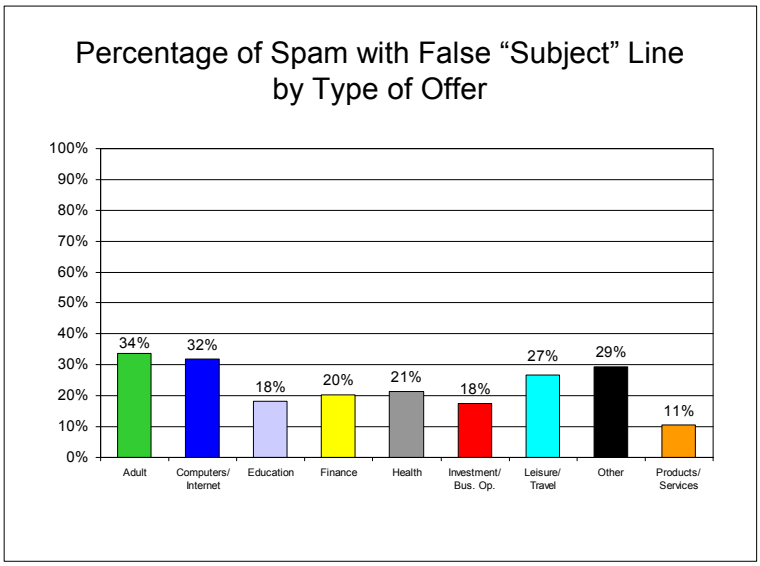
Twenty-two percent of spam analyzed contained false information in the "Subject" line.

Of the spam containing signs of falsity in their "Subject" lines, nearly one-third contained a "Subject" line that bore no relationship to the content of the message. These false "Subject" lines were designed to lure consumers into opening the messages, expecting to see content related to the representations in the "Subject" lines. Forty-two percent of the spam containing false "Subject" lines misrepresented that the sender had a personal or business relationship with the recipient.



Forty-two percent of spam containing misleading "Subject" lines misrepresented that the sender had a personal or business relationship with the recipient.

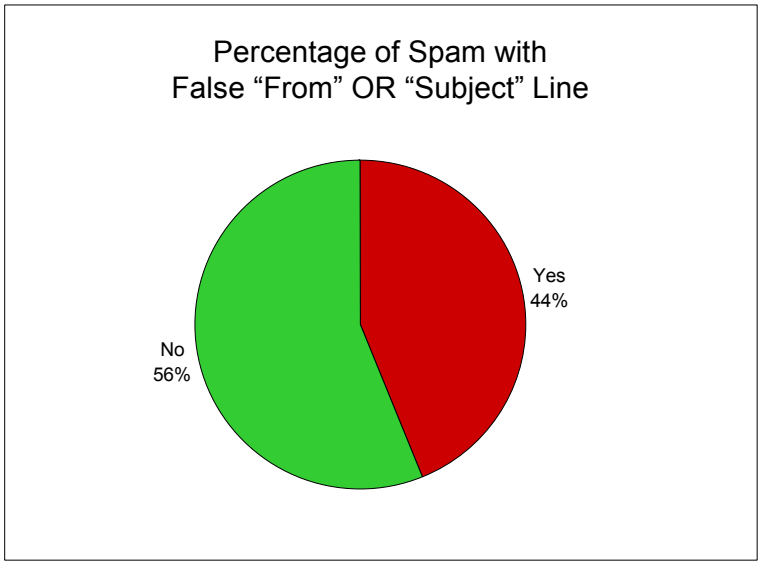
While false "Subject" lines were found in all types of offers, over one-third of "adult" offers appeared to misrepresent the content of the message.



One in every three "adult" spam messages reviewed by the FTC contained false information in the "Subject" line.

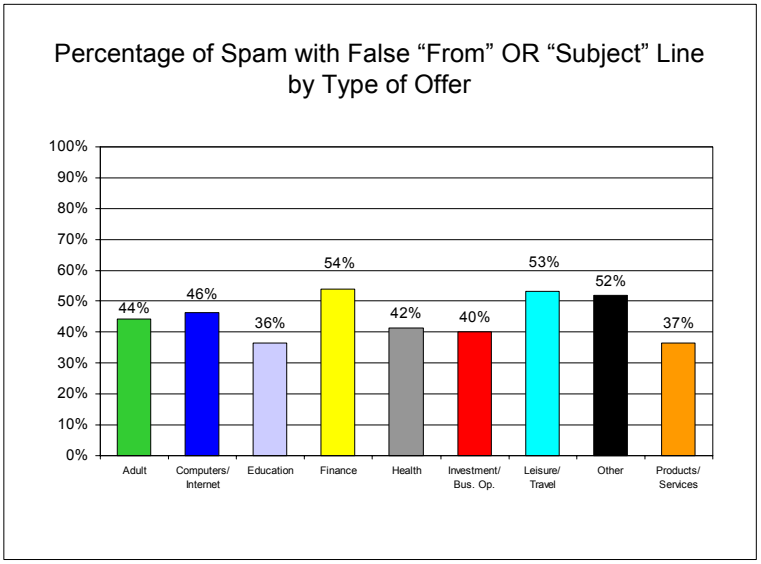
V. FALSITY IN "FROM" OR "SUBJECT" LINES

Forty-four percent of spam analyzed by FTC staff contained hallmarks of falsity in either the "From" line or "Subject" line.



Forty-four percent of spam reviewed by FTC staff contained false information in the "From" or "Subject" lines.

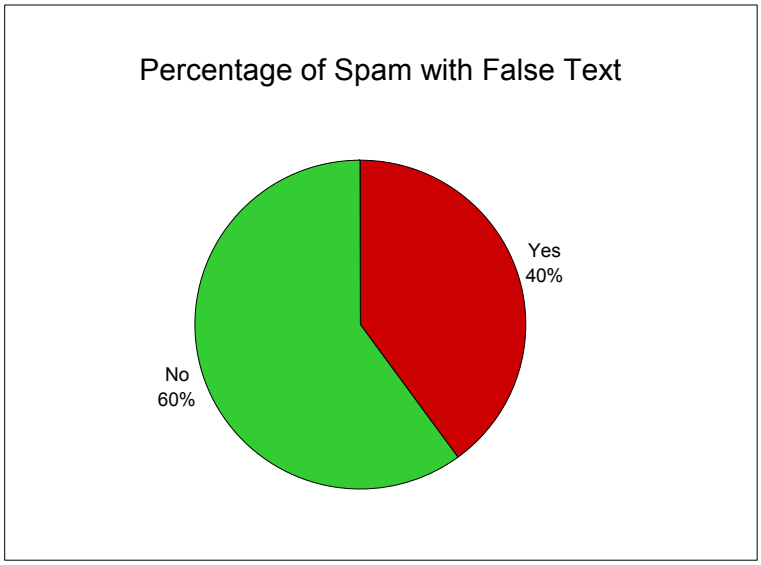
All types of spam in the sample analyzed by FTC staff contained indicators of falsity in the "From" or "Subject" line, with incidence rates ranging from a low of 36.4% for education-related UCE to a high of 53.9% for finance-related spam.



Over half of finance-related spam analyzed by the FTC contained false "From" or "Subject" lines.

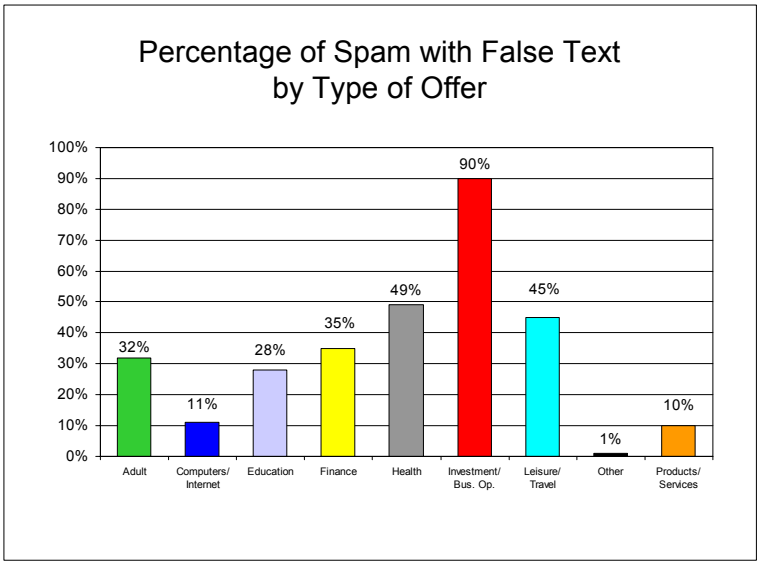
VI. FALSITY IN MESSAGE TEXT

Using expertise gleaned from past law enforcement actions and its own research, FTC staff identified specific representations that were likely to be false. Staff then analyzed each spam message in the sample to determine whether its text bore any of the enumerated hallmarks of falsity. Approximately 40% of the messages had at least one indication of falsity.



Forty percent of spam studied contained signs of falsity in the body of the message.

The incidence of likely false claims in the text of spam varied considerably among types of offers. Ninety percent of UCE in the sample that advertised investment and business opportunities contained signs of falsity.

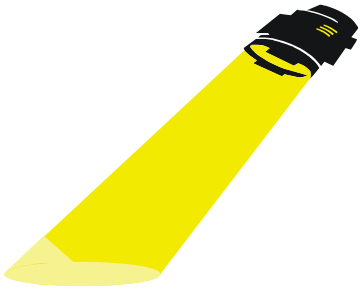


Ninety percent of spam concerning investment and business opportunity offers analyzed by the FTC contained likely false claims.

Many of the Investment/Business Opportunity messages analyzed for this study could be categorized as "chain letter" messages, and many others advertised some other form of "effortless income."

Chain letter and effortless income offers are frequently marketed through UCE.

Spotlight on:



"Chain Letter" Spam

What the "chain letters" say:

- "Read on. It's true. Every word of it. It is legal. I checked."

What to watch out for:

- Chain letters may try to win your confidence by claiming that they're legal, and even that they're endorsed by the government. Nothing is further from the truth.

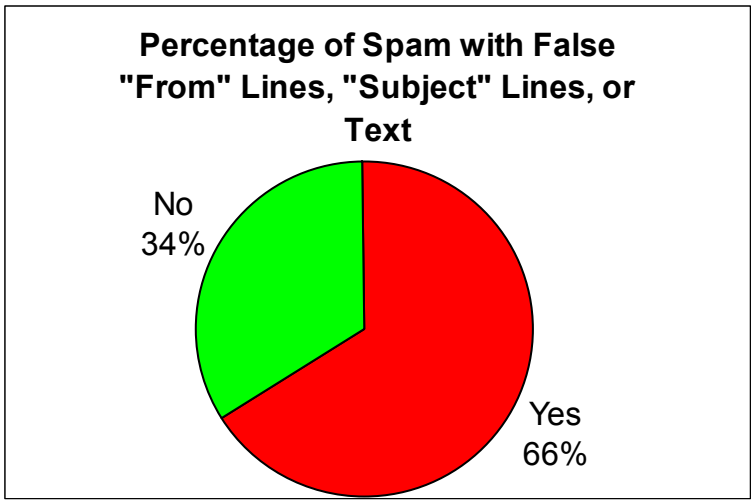
Of the spam analyzed, 48% marketing healthcare products and 47% marketing travel or leisure products contained signs of falsity in the text of their messages.

Other topics generating a significant percentage of messages with indicators of falsity included those involving health (48%) and leisure/travel (47%). Common "health" spam messages advertised weight loss products and intimacy aids; common "leisure/travel" spam messages offered prize and vacation promotions.

VII. FALSITY IN "FROM" LINE, "SUBJECT" LINE,

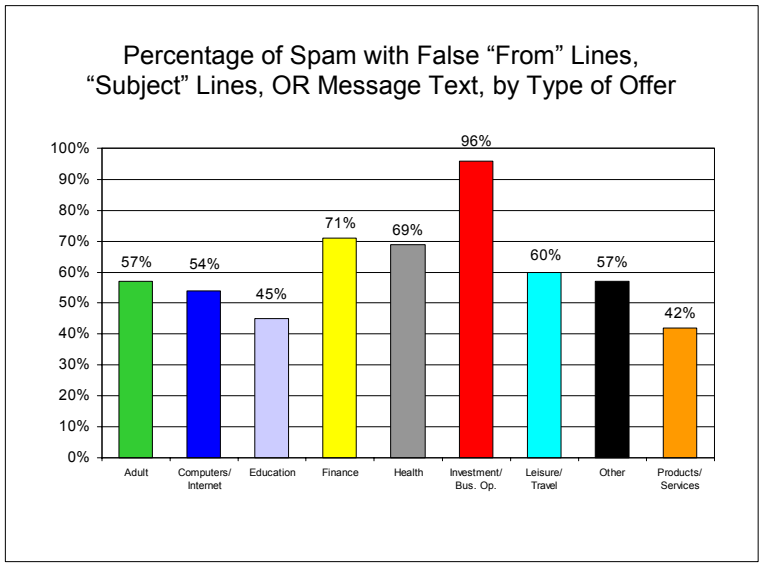
OR MESSAGE TEXT

Sixty-six percent of spam analyzed by FTC staff contained indications of falsity in their "From" lines, "Subject" lines, or message text.



Sixty-six percent of spam analyzed contained false "From" lines, "Subject" lines, or message text.

All types of spam in the sample contained indications of falsity in the "From" or "Subject" line or in the message text, with falsity rates ranging from a low of 42% for spam involving the sale of products and services to 96% for spam offering investment and business opportunities.

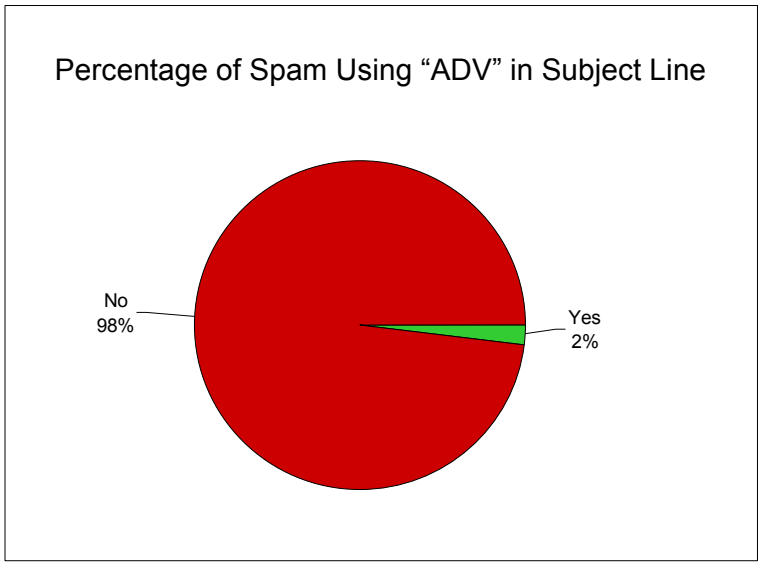


Ninety-six percent of spam concerning investment and business opportunities contained false "From" lines, "Subject" lines, or message text.

VIII. USE OF THE "ADV:" LABEL IN "SUBJECT" LINES OF MESSAGES STUDIED

Several states have enacted laws in recent years requiring senders of spam to begin every subject line with the phrase "ADV:" (an abbreviation used to identify advertising) in messages sent to recipients of those states. FTC staff's study of a sample of messages found that compliance with this labeling requirement was sparse.

Two percent of the spam analyzed contained the "ADV" label in the subject line, which is required by several state laws.



IX. MESSAGES REQUESTING RECIPIENTS' PERSONAL INFORMATION

The spam study showed that messages rarely requested recipients to submit personal information in responding to the senders' offers. In analyzing spam regarding this feature, staff distinguished between information that is public and readily available, such as the sender's name and address, and information that is not public or is not readily available, such as the sender's bank account number. The latter type of personal information consists of data that can lead to identity theft or other monetary harm if it falls into the wrong hands; the FTC advises consumers to guard this information carefully. Only 14 of the UCE in the sample requested such personal information. Ten of these 14 messages also contained indicators of falsity in the "From" line, "Subject" line, or body of the message.

While relatively few spam in the study asked the recipient to submit personal information, those messages requesting such information typically contained signs of falsity.

Spotlight on:

"Nigerian" Spam &
Personal Information

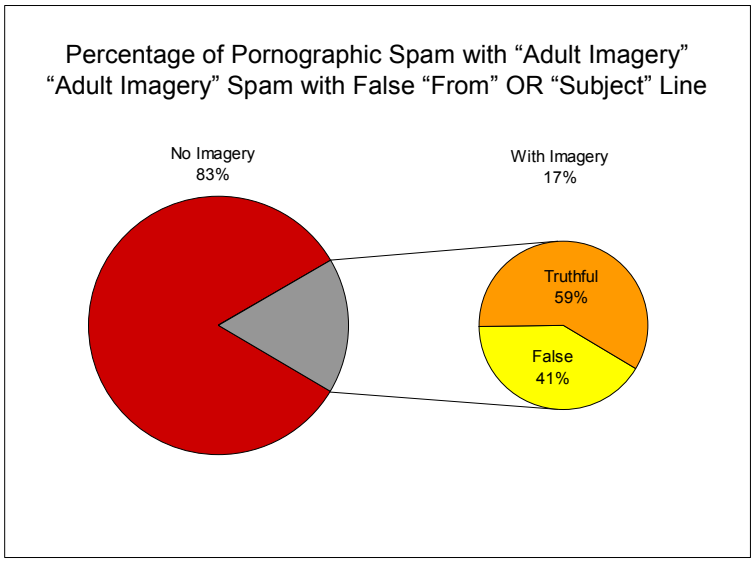
- These messages may ask for your bank account number–purportedly so the sender can wire you millions of dollars.
- If you respond and provide your account information, you will receive nothing–and the sender will have access to funds in that account.

X. USE OF ADULT IMAGERY IN OFFERS FOR PORNOGRAPHY

Consumers and lawmakers have repeatedly expressed concern over sexually explicit images contained in spam, principally because the images may be accessible to children. To help determine the scope of this issue, FTC staff analyzed the prevalence of pornographic imagery in the Harvest Database and the database of spam received in FTC employees' inboxes. (Because many consumers who forwarded their spam to the UCE Database did not send the spam in an HTML-enabled format, the UCE Database sub-sample was excluded from this particular analysis). A message was considered to have "adult imagery" if the image appeared automatically (without requiring the consumer to hyperlink to a web page) and the image contained nudity.

Seventeen percent of pornographic offers in the spam analyzed by FTC staff contained "adult imagery." Over 40% of these pornographic spam messages contained false statements in their "From" or "Subject" lines, making it more likely that recipients would open the messages without knowing that pornographic images will appear.

Seventeen percent of spam advertising pornographic websites included "adult images" in the body of the message.



XI. METHODOLOGY

For this study, FTC staff analyzed UCE from three sources – the UCE Database (approximately 450 sample messages), the Harvest Database (approximately 450 sample messages), and spam received in official FTC inboxes (approximately 100 sample messages). The UCE Database and Harvest Database samples were drawn from messages received during the last six months of 2002. The UCE messages were collected for this study using random selection protocols established by the FTC Bureau of Economics. To enable future internal analysis of spam not blocked by the FTC's internal computer systems, the data sample was supplemented with 100 pieces of randomly-selected UCE received by FTC employees during March 2003.

Forty-one percent of spam containing "adult imagery" contained false information in their "From" or "Subject" lines.

The UCE Database contains spam forwarded to the Commission by members of the public. Consumers currently contribute about 130,000 messages per day to the UCE Database, and a total of 11,184,139 messages were forwarded to the FTC's UCE Database during the time period from which the study's sample was drawn. The volume of messages in the UCE Database makes it likely that this data source provides a fairly representative look at the

types of messages that many consumers receive. Nonetheless, the email in the database may be skewed because contributors are likely to be knowledgeable about spam or have a dismal view of UCE.

The Harvest Database consists of 3,651 messages received by FTC undercover email accounts that were established as part of its email harvesting study. As part of the Harvest study, the FTC and its law enforcement partners established 250 email accounts and posted these email addresses to 175 different locations on the Internet. Specific email addresses were posted on newsgroups, message boards, chat rooms, instant messaging services, email service directories, web pages, domain name "whois" information, online resume services, and online dating services. FTC staff then tracked email received by each of the 250 email accounts.

While spam contained in the Harvest Database does not suffer from the same potential "contributor" biases as the UCE Database, it may not be fairly representative of the range of spam offers that consumers receive. The database contains messages sent by marketers who use harvesting programs to obtain email addresses. Many marketers eschew using harvesting programs and obtain email address lists in other fashions.

The internal FTC spam database may suffer from the same potential biases as the UCE Database. Commission staff voluntarily contributed the spam they received in their FTC inboxes for analyses. Contributors may be those employees most annoyed with spam. Moreover, the FTC employs email filtering mechanisms that likely affect the representativeness of this sample.

To overcome the potential biases in each of these data sets, the data was combined into a single database. The study's results provide a snapshot of approximately 1,000 pieces of spam drawn from a variety of sources available to FTC staff. It is unknown whether a random sample of all spam sent in the stream of commerce would yield the same findings.

XII. CONCLUSION

This study represents a snapshot of spam, as viewed through random samples of three data sets available to FTC staff. Because all vehicles of commerce, including spam, are in constant motion, this snapshot may not provide a complete picture of the incidence of false claims in spam.

Reviewing this snapshot, FTC staff found that UCE for Investment/ Business Opportunity, Financial, and Adult offers accounted for over half of all messages. When analyzing the prevalence of false claims, FTC staff found indicators of falsity in the "From" lines, "Subject" lines, or content of two-

thirds of the messages. Furthermore, this study found that the use of the "adv" (advertising) label by senders of spam was almost non-existent. Finally, the study found that 41% of spam depicting nudity contained indicators of falsity in their "From" or "Subject" lines.

Future studies should be designed to identify changes in the types of offers being made through spam and the frequency of signs of falsity appearing in the "From" lines, "Subject" lines, and content of UCE.