FIGHTING MAIL ORDER FRAUD AND THEFT

Best Practices for the Mail Order Industry

REFERENCE GUIDE

Publication 309, January 1999

UNITED STATES POSTAL SERVICE®

Fighting Mail Order Fraud and Theft

Publication 309

January 1999
Transmittal Letter

A. Explanation. This is a new publication, prepared jointly by the U.S. Postal Inspection Service, the Direct Marketing Association (DMA), the Advertising Mail Marketing Association (AMMA) and postal representatives. It provides guidelines for the mail order industry on how to protect their mail and reduce losses from mail order fraud and theft.

B. Distribution. This publication was initially distributed to Inspection Service mail order coordinators, the DMA, the AMMA and designated Postal Service area and district personnel.

C. Effective Date. Information in this publication is effective upon receipt.

D. Additional Copies. Additional copies may be ordered as follows:

1. **Postal Service Customer** Relations account managers may place orders for this publication through the Field Force Inventory catalog on the Customer Relations Connection Intranet Web site. Request Publication 309, *Fighting Mail Order Fraud and Theft,* and state the quantity you need.

2. **Other Postal Service personnel** may place orders for this publication by submitting PS Form 7380, *MDC Supply Requisition*. MDCs may only fulfill orders received from Postal Service or Postal Inspection Service personnel.

3. **Members of the mail order industry** may order copies of this publication by contacting their Customer Relations account manager or the mail order coordinator at their local Postal Inspection Service office.

E. Comments and Questions. Address any comments or questions to:

CONGRESSIONAL & PUBLIC AFFAIRS
US POSTAL INSPECTION SERVICE
475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-2175

The following Mail Order Task Force advisors contributed their knowledge and expertise to the creation of this guide:

Sean Buckley
Doubleday Direct
401 Franklin Ave.
Garden City, NY 11530-5945
(516) 873-4175

Sandy Freund
Gevalia Kaffe
555 South Broadway
Tarrytown, NY 10591-6301
(914) 335-4206

Marsha Goldberger
Direct Marketing Assn., Inc.
1111 19th St. NW, Suite 1100
Washington, DC 20036-3603
(202) 955-5030

Darlene C. Hartman
Current Checks, Inc.
P.O. Box 35370
Colorado Springs, CO 80935-5370
(719) 531-3870

Carla Harding
Time Life Inc.
777 Duke St.
Alexandria, VA 22314-3621
(703) 838-7446

Jim Leslie
The Franklin Mint
Franklin Center, PA 19091-0001
(610) 459-6185

Julie Moorhead
Fingerhut, Inc.
53 McLeland
St. Cloud, MN 56395-2076
(320) 654-7493

Karen Root
Rodale Press
33 East Minor St.
Emmaus, PA 18098-0099
(610) 967-8142

Kathy Siviter
Advertising Mail Marketing Assn.
1901 N. Ft. Myer Dr. Ste. 401
Arlington, VA 22209-1609
(703) 524-0096

TABLE OF CONTENTS

CONFIDENCE IN THE MAIL

For more than two centuries, the U.S. Postal Inspection Service has been committed to preserving the public's trust in postal services. Today, it has evolved into a modern law enforcement agency whose mission is to ensure the integrity of the mail and the Postal Service by providing investigative, security, audit and preventive services and by enforcing federal statutes that protect the mail, postal employees, customers and assets. It is committed to increasing customer confidence in the use of the mail as a safe, secure and reliable means of commerce and communications.

The Postal Inspection Service, as part of its effort to preserve and enhance the public's confidence in the mail, has partnered with the financial services, manufacturing and direct marketing industries on behalf of the U.S. Postal Service to form three task forces: Credit Card Mail Security, Rebate Fraud and Mail Order Security. The task forces include Postal Inspectors, major customers, suppliers from the targeted industries and other postal representatives. Each task force helps to reduce mail fraud, theft and processing problems by identifying and exchanging information on best practices, fraud trends and loss-prevention techniques; and to develop improved processes and procedures. All three initiatives also focus on facilitating criminal investigations and prosecution where warranted.

Created in 1992, the Credit Card Mail Security Task Force has dramatically reduced nonreceived issued (NRI) credit card fraud losses by 68%, while credit card purchases have increased more than 86%. One of its first efforts was the development of the 1-800 activation process for new credit cards, a program that has revolutionized industry practices. It produced two "best practice" manuals: *Detecting and Preventing Credit Application Fraud* and *Detecting and Preventing Account Takeover Fraud*. The Task Force also contributes information to the Mail Theft Reporting System, a proprietary database, which facilitates fraud detection and analysis.

In 1995, the Postal Inspection Service teamed with the coupon rebate industry to combat mail-in rebate fraud. The group's efforts reduced fraud by an estimated $100 million in 1997. Like the Credit Card Task Force, the Rebate Fraud Task Force has a number of ongoing initiatives, including a shared database of suspected fraudulent submissions, and has developed a best practices resource guide: *Promotion Industry Guidelines for Mail-In Offers*.

The Mail Order Task Force

The direct marketing industry has enjoyed increasing success in offering products and services through the U.S. Mail. In 1996, the Postal Inspection Service and the direct marketing industry created the Mail Order Task Force to facilitate this continued success by joining together to prevent and detect fraud and theft. The mission statement of the Task Force is "Reduce mail order nonreceipt and fraud losses in measurable terms."

In a pilot program, the Task Force has already reduced nonreceipt losses by 10% to 15% for direct marketing companies experiencing mail processing problems. Prompt identification and criminal investigation of mail theft and fraud promises to reduce losses further. The Task Force is also working with companies to create an industry-wide database to maintain fraud statistics and more quickly identify perpetrators.

This reference guide is intended to provide direct marketing professionals with best practices that have been identified by the Task Force to help them recognize and prevent mail order fraud and nonreceipt. By working together, direct marketers and the U.S. Postal Inspection Service can successfully reduce mail order losses as well as target, pursue and shut down illegal activities. This will reduce the loss of money and time, improve customer service and improve confidence in the mail.

KENNETH J. HUNTER
CHIEF POSTAL INSPECTOR

UNITED STATES POSTAL SERVICE

TO THE DIRECT MARKETING INDUSTRY

The U.S. Postal Inspection Service is pleased to be a partner with the direct marketing industry in this joint effort to combat mail order fraud and nonreceipt. Both fraud and nonreceipt are costly to the direct marketing industry. Mail theft can also have a negative impact on customers' desire to order by mail. The Mail Order Task Force was created to reduce and prevent such losses. Through this partnership, Task Force representatives work on a variety of projects focusing on education and prevention, as well as on administrative, civil and criminal remedies. By examining mail fraud, theft, nonreceipt and mail processing issues, improvements can be made to increase customers' confidence in the U.S. Mail.

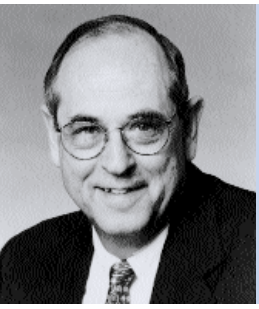
One major accomplishment of the Mail Order Task Force is this reference guide. Combining the talents of industry and law enforcement, this guide presents an overview of mail order processing, various types of fraud and a useful summary of best business practices, including prevention measures and corrective actions.

The adoption of voluntary guidelines, as well as the aggressive pursuit of those individuals intent on abusing the system, will produce positive results. By continuing the work already in progress, together we can further reduce mail order fraud, theft and nonreceipt.

K. J. Hunter

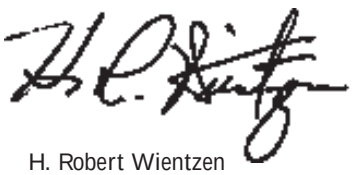
A MESSAGE FROM THE DMA AND AMMA

The Direct Marketing Association (The DMA) is pleased to be an active participant in the joint effort to prevent fraud against mail order sellers. We have been a part of the Mail Order Task Force since its inception because of our belief that working together as an association and as individual members with the U.S. Postal Inspection Service is the most comprehensive way to fight fraud and reduce the considerable losses that all marketers experience.



Fraud in the marketplace is a serious matter when consumers are defrauded by mail order companies. It negatively impacts confidence in direct marketing as a legitimate way to conduct business. But as you know, fraud is also perpetrated against legitimate businesses and can significantly impact the bottom line. The U.S. Postal Inspection Service has extended extraordinary resources toward learning the scope of losses experienced by mail order companies and developing concrete ways to prevent and reduce such losses.

In this best practices reference guide you will find information on how to recognize and prevent fraud. Sample letters to warn suspected criminals and recommendations for improving employee, plant and transportation security are also included to enhance your fraud and theft prevention efforts.



H. Robert Wientzen
President and CEO

The Advertising Mail Marketing Association (AMMA) has been working closely with the U.S. Postal Inspection Service and others to help prevent mail order fraud and theft. Fraud costs our industry billions of dollars in lost sales and revenue, and it reduces everyone's confidence in the mail as a means for communicating and doing business. This benefits no one.

There are, however, sensible steps that every business mailer can take to prevent fraud from occurring or to nip it in the bud as soon as it appears. The U.S. Postal Inspection Service, in cooperation with our industry-sponsored work group, has put together this best practices reference guide to help address these concerns. Here you'll find the necessary tools to identify and combat the fraud and nonreceipt that may be costing your company dearly. In addition, you'll find sample letters, legal notification forms, and a glossary of terms that can serve as ready references. Lists of "warning signs" are included as a way to red flag potential fraud.

Here's your chance to "take a bite out of crime."

Gene A. Del Polito
President

DIRECT MARKETING AND FRAUD

Americans are increasingly attracted to the convenience and reliability of home shopping. Nearly seven out of ten U.S. adults made a purchase by mail or by phone in 1995. Direct marketers are making it easier to order by applying new technologies and databases and by offering innovations like express delivery, guarantees, and credit availability. According to a Direct Marketing Association-commissioned study, direct marketing sales in the United States approached $1.2 trillion in 1997. More than $684.6 billion in sales were made to consumers. In addition, $541.6 billion in sales were made to businesses. Unfortunately, losses from fraud, nonreceipt and bad debt can reach billions of dollars in the United States alone.

The Terms

As there is not always complete agreement on mail order fraud terminology, the following definitions will apply for the purposes of this guide:

- **Fraud** is the intentional obtaining of merchandise or something of value without payment and typically involves deception or misrepresentation of material facts. A mail fraud violation occurs when the U.S. Mail is an integral part of a fraud scheme. The Mail Fraud Statute (a felony) is contained in Title 18 of the U.S. Code, Section 1341. This statute is the oldest consumer protection law in the United States. There are also certain civil administrative statutes available to help combat fraud.

- **Nonreceipt losses** result from a customer claiming that (a) merchandise was not received; (b) merchandise was ordered, received, and then returned to the mail order company, which did not receive the return; or (c) merchandise was neither ordered nor received, but they have received a bill. Nonreceipts also may occur as a result of damage in handling, theft during shipment, or theft after delivery.

- **Bad debt** is generally defined as an uncollectible accounts receivable in a business context. Losses from mail fraud and nonreceipt contribute to overall bad debt and can seriously affect the credit status of companies that experience such losses.

A Growing Problem

Mail order fraud varies from simple incidents involving a single customer name and address to complex fraud schemes with multiple names and addresses and organized groups of criminals. Some losses result when mailed articles are stolen out of the U.S. Mail before delivery or are otherwise reported "not received" by the addressee. Others result from poor packaging or improper mailing addresses.

Without proper internal controls and prevention measures in place, small losses may quickly grow into large ones. It is also important to recognize that a particular fraud scheme directed against one mail order company may result in relatively small losses for that company; however, other companies may also have been victimized by the same fraud scheme. Combined aggregate losses attributed to the same fraud scheme may be very large. Teamwork among direct marketers and the Postal Inspection Service is a potent weapon in fighting such schemes and preventing them from spreading.

A Postal Inspection Service survey of 22 mail order companies conducted in 1996 revealed that 94% of the companies surveyed believed that mail order fraud and nonreceipt were growing problems, and 70% had major initiatives underway to counteract them. The companies recognize the following fraud schemes as most common in the industry:

- Identity theft and account takeover fraud
- Credit application fraud
- Claims paid fraud
- Overpay refund/bad check fraud
- False damage claim fraud
- Bill to/Ship to fraud
- Change of address fraud
- True name fraud
- Claims returned fraud
- Nonreceipt fraud
- Multiple names/addresses fraud
- Check fraud
- Deceased customer fraud

This reference guide provides a ready reference for recognizing, flagging, and reporting such activities.

Without watchful attention by direct marketers and the Postal Inspection Service, criminals can perpetrate a mail fraud scheme, cover their tracks, and move on before detection and apprehension. It is important to conduct pre- and post-promotion reviews to ensure the integrity of the fraud prevention efforts and systems.

Pre- and Post-Promotion Reviews

Due to the wide variety of procedures within the industry, direct marketing companies should use a standardized review to protect the interests of the parties involved and to assist law enforcement officials in possible investigations. The more attention paid during the review stage, the less likely a direct marketing company will honor fraudulent submissions. Below is a list of reviews that should be completed for all orders.

Phone, Mail and Internet Order Entry

The most important place to look for fraudulent submissions is at the checking station where mail order offers are taken, opened and verified. Make sure data-entry staff is aware of the warning signs for mail, phone and Internet order fraud. See Warning Signs and Specific Prevention Techniques, pages 16 through 21, for more information.

Verifying Telephone Numbers

If telephone numbers are a special condition of the promotion, software can be used to verify the telephone number against the identity of the individual who submits a mail order. The software is available on CD-ROM and can be purchased at computer stores or through computer catalogs. Both address and telephone information inquiries can be made with such programs.

Verifying Addresses

Check each name and address on a mailing list by using only USPS Coding Accuracy Support System (CASS) certified address matching software and format it into Postal Service standards following the guidelines in Publication 28 *Postal Addressing Standards*.

For more information on USPS approved address matching software and *Postal Addressing Standards* visit the USPS website (www.usps.gov) or write:

Support Programs Department
National Customer Support Center
United States Postal Service
6060 Primacy Pkwy., Suite 201
Memphis, TN 38188-0001
(800) 238-3150, ext. 4495

On-Line Lookup System

On-line lookup systems are useful in determining whether to honor a customer order. A lookup system requires that a list of respondents, grouped by offer, be maintained for three months to a year (depending on data storage capacity). Company records should indicate whether a response was honored and, if not, the reason why. The on-line lookup system provides information to alert to a possible fraud. All on-line systems should have CASS address matching software attached. This will allow you the opportunity to validate the address while the customer is on the line.

Duplicate Order Elimination

Computerized duplicate elimination, used by most direct marketing companies, automatically eliminates duplicate orders to the same name or address. While it does not constitute a total fraud prevention package, when used in conjunction with other tools and controls it helps identify those who use the mail to defraud and raises the cost-efficiency of orders.

In selecting a duplicate elimination program, remember the tighter the parameters, the more likely a legitimate consumer may be refused an order. No program is perfect. Each direct marketer must decide whether it wants to err on the side of achieving a higher number of matches at the risk of offending some consumers or letting some fraudulent

An alert employee of a large direct marketer of mail order tapes, CDs and recordings noticed an unusual number of new orders going to post office boxes in the Washington, DC, area. When bills for the merchandise became overdue, the company notified the U.S. Postal Inspection Service of suspected fraud. Other companies began reporting the same suspicious pattern. Within months, the Service uncovered a scheme in which eight individuals, using fictitious names and false credit information, received merchandise at more than 200 locations in the Washington area. The stolen goods were then shipped to Nigeria for resale. Total losses to mail order companies reached $1.5 million. Six of the individuals have been convicted of mail fraud, money laundering and conspiracy and sentenced to federal prison. U.S. Attorney Lynne A. Battaglia, District of Maryland, praised the extraordinary level of cooperation provided by the mail order merchandise companies and the U.S. Postal Inspection Service in bringing these crimes to light and to a speedy conclusion.

orders slide through. Post-promotion analysis of duplicate information helps detect and log fraud after orders are fulfilled.

Multiple Order Elimination
Employing a system that prevents multiple orders from the same customer being shipped without payment helps reduce possible fraud losses.

Loss Prevention Files
Maintain loss prevention files to track bad addresses, bad debt, orders claimed not received, merchandise not returned (claims returned), insufficient funds checks, multiple names at the same address, credit card denials and similar negative information.

Delivery Sequence File (DSF)
The DSF is a USPS licensed computerized file that contains all USPS delivery addresses and can be used to detect fraudulent and duplicate addresses. Processing your mailing list through a DSF process can also provide full address standardization and meet all CASS address matching requirements for postal discounts. The file contains ZIP+4, carrier route, delivery sequence, delivery type, commercial mail receiving agency locations and seasonal addresses.

Commercial Resources

A number of commercial fraud prevention technologies are available to help direct marketing organizations combat fraud. In general, the systems take information from applications and order forms, and compare it to external databases and probability models for fraud to produce warning profiles for potential instances of fraud. These computerized programs can be monitored by outside professionals or managed in-house.

Because of the diversity of vendors and variety of products and information in the marketplace, available programs, software and services are referred to only in general terms. It is important to note that many fraud prevention techniques can be automated. Each company should use its best judgment to research and identify all possible resources that can assist in the effort to reduce fraud.

ECOA and Regulation B Compliance

Careful screening and consultation of databases will result in denial of credit to a small portion of those who respond to the offers of direct marketers. The Equal Credit Opportunity Act (ECOA) and Regulation B (Reg B) require a creditor that declines an application to notify the applicant of the action taken within 30 days of having received the completed application ("adverse action notice").

The Fair Credit Reporting Act (FCRA) also requires a creditor to disclose when it has based its decision to decline credit for personal, family and household purposes in whole or in part on information from a source other than the applicant or its own files. If information is obtained from a credit bureau, the creditor must disclose the name and address of the credit reporting agency.

Requirements

Creditors should review ECOA Reg B to be sure that an adverse action notice identifying the credit bureau is required in the situation at hand to reduce damages and losses associated with the submission of fraudulent credit applications and to protect the general public from being victims.

Note: The following requirements for the letter apply, with the assumption that a real person is submitting the application for a legitimate purpose and that the applicant is providing credit information about himself or herself. None of these is true in the case of a fraudulent application.

1. The adverse action notification requirement applies when a creditor has received a completed application from an applicant. Reg B defines an applicant as a person who requests an extension of credit from a creditor. An application is defined as an oral or written request for an extension of credit that is made in accordance with procedures established by a creditor for the type of credit requested.

2. The requirement to supply the name and address of the consumer reporting agency providing the credit report applies when credit is denied for personal, family, or household goods.

3. When a creditor receives an application, the creditor may verify the application by direct contact with the applicant in any situation identified by the creditor as a potential fraud before the credit decision is made. When it is determined that the true creditworthy individual did not apply for the credit, there is no requirement under Reg B or the FCRA to send a written notification to the perpetrator.

Alternative Actions

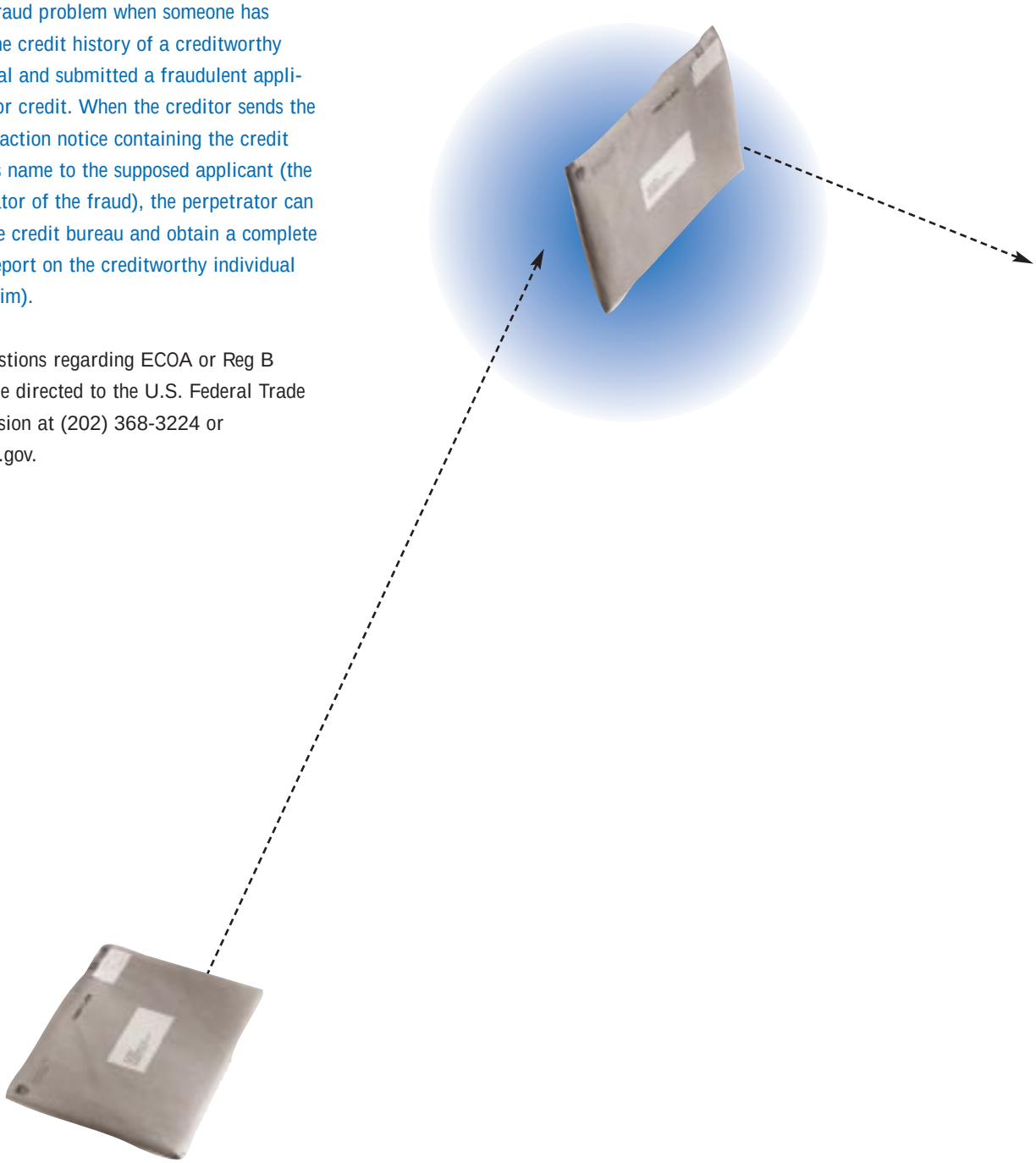
If the creditor is highly suspicious of the application, and its attempts to contact the applicant are unsuccessful, the creditor may want to send a letter to the applicant:

- advising that attempts to contact the applicant for verification of application information have been unsuccessful; and
- requesting the applicant to contact the creditor within a specified period of time.

The letter should not contain reference to the applicant's Social Security number. In addition, the creditor's contact telephone number should be in the Fraud Security unit (preferably a phone that is answered in a neutral fashion, not "Fraud and Security") to allow appropriate investigation of the request. Direct marketing companies should check with their legal counsel to ensure that procedures adopted comply with the law and are not in conflict with other company policies.

NOTE: The requirement to notify the applicant when credit has been denied can aggravate a fraud problem when someone has stolen the credit history of a creditworthy individual and submitted a fraudulent application for credit. When the creditor sends the adverse action notice containing the credit bureau's name to the supposed applicant (the perpetrator of the fraud), the perpetrator can go to the credit bureau and obtain a complete credit report on the creditworthy individual (the victim).

Any questions regarding ECOA or Reg B should be directed to the U.S. Federal Trade Commission at (202) 368-3224 or www.ftc.gov.



FRAUD PREVENTION BEST PRACTICES

Below are some general fraud prevention techniques that have proven effective in the industry. More specific techniques for fighting mail order fraud via telephone, mail-in and on-line orders are offered in the next chapter.

Training and Awareness

- A well-informed staff is the best protection against losses from fraud.
- Educate front-line staff on recognition factors that indicate fraud.
- Encourage rapid reporting of new or actionable fraud cases.
- Train order entry personnel to ensure the application has been thoroughly completed.
- Offer rewards to astute order entry personnel who identify fraud attempts.
- Communicate the likelihood of fraud to marketing, customer service and credit and collections staff.
- Provide key personnel with the skills and tools to investigate fraud.

Reviews and Databases

- Use an Address Verification System (AVS) on all orders received.
- Create an in-house fraud database to identify suspected fraud addresses, names, telephone numbers, etc.
- Review fraudulent applications to determine flaws in the screening process and opportunities to close gaps. Learn from prior experience.
- Monitor established accounts for known patterns.
- Establish normal parameters for customers' behavior to recognize abnormal events more easily when they occur (e.g., ordering pattern changes).
- Use external data sources to confirm customer-provided data.
- Establish a process to control results, restitution and status of pending cases.
- Conduct a visual review of all applications.
- Look for obvious misspellings throughout the order form.
- Identify home and/or business addresses, post office boxes or addresses with "suites" indicating possible use of a commercial mail receiving agency (CMRA) or answering service.
- Track unusual response patterns to various promotions.
- Track customer ordering and payment patterns by ZIP Code to determine unusual delinquency and bad debt ratios.

- Do routine audits of charge-backs, returned checks, customer allowances and bad debt charge-offs to identify patterns.
- Check for response trends disproportionate to pieces mailed.
- Track trends using fraud management system software to recognize when and where fraud is increasing.

Investigation and Reporting

Direct marketing companies that are successful detecting fraud and theft utilize in-house investigators and a standard process. When warranted, a theft or fraud problem can be referred to the Postal Inspection Service under the process described on pages 24 through 26.

- Provide an easy method to forward potential fraud activity to an in-house investigator.
- Commit to legal remedies through cooperation with prosecution.
- Commit to court appearances.
- Develop internal checks to guard against employee theft/fraud.

Fraud Management System

To optimize fraud prevention techniques, direct marketers should gather information from many key data sources and incorporate that information into the review process. To the right is a sample of how to develop an integrated fraud management system that takes all automated systems into consideration and offers suggestions on when to apply them to the decision-making process.

A CLOSER LOOK

In 1995, a man began renting mailboxes at post offices and commercial mail receiving agencies (CMRAs) throughout northeastern Pennsylvania. In two years he had amassed approximately 40 addresses and created a failure-to-pay fraud scheme against major direct marketers. By acting upon the warning signs and using proven fraud prevention techniques, the companies were able to alert the Postal Inspection Service, which apprehended him. In 1997, he pled guilty and was sentenced to two years in prison and $45,564 in restitution.

FRAUD MANAGEMENT SYSTEMS OVERVIEW

Credit Approved Orders

Account Variables

Order Level Variables

Address Variables

External Consumer Data Validation

Consolidation

Customer Service Transactions

High-Risk Database

Fraud Probability Scoring Module

External Sources*

Fraud Indicators?

Yes

No

Manual Review (if score indicates risk)

Release Order

Request Additional Information

Request Prepayment

Fill or Cancel Order

*See page 10, Commercial Resources, for more information.

WARNING SIGNS AND SPECIFIC PREVENTION TECHNIQUES

It is at the front lines — the phone call, mail order form or on-line order — that the direct marketing industry stands the best chance of recognizing and fighting such crime. Losses can be significantly decreased by learning to spot the warning signs of fraud, using the correct prevention techniques, and ensuring that everyone at the company is aware of these signs.

The warning signs should serve as alerts for further investigation. Any one incident, or even a combination of incidents, is not proof but an indication of the possibility of fraud. In addition, some of the warning signs have been developed under the assumption that order and customer tracking systems are already in place.

The list of mail order warning signs and prevention techniques can be distributed to company employees and posted at their work areas as a ready reference for recognizing potential incidences of fraud. Attached to this list should be the company's internal reporting procedures, so that prompt and effective action can be taken in identifying fraudulent practices. By spotting mail order fraud early, reporting it promptly and correctly to the Postal Inspection Service, and working with the Service to prosecute such crime, industry losses will be minimized and consumer confidence in shopping by mail will remain high.

Mail-In Order Forms

Warning Signs

Many of the following signs apply to all types of orders and applications.

Personal Information

Name

- Same or similar names on multiple orders.
- Unusual name configurations, such as first names used as both given and surname (e.g., John N. James, Dennis L. George).
- Unusual names that are difficult or nearly impossible to pronounce (e.g., Opriglsn Ameolinaduni).
- Names of known personalities (e.g., John Wayne, Marilyn Monroe).
- Name reversals between the applicant line and the signature line.

Address

- Extensive use of post office boxes or box numbers.
- Same or similar addresses on multiple orders.
- Same or similar addresses in adjoining ZIP Codes.
- Multiple orders for multi-family dwellings.
- Multiple names to a post office box or same name to multiple boxes in the same post office.
- Multiple variations of box numbers or apartment alpha codes.
- Addresses with suite numbers (may indicate use of a CMRA).
- Dwelling-type errors (e.g., apartments in single-family dwellings).
- Nonsequential apartment numbers.

Phone

- Phone number and area code not consistent with address.
- Frequent callers and different orders from the same phone number.

Payment/Shipment Information

- Unusual use of alpha values (such as XX or E) in financial information columns.
- Colons in dollar amounts.
- First four digits of VISA or MasterCard do not coincide with issuing bank identification numbers.
- Reference account numbers abbreviated/truncated.
- Bill to/Ship to addresses are different.
- Express delivery (must have by).
- Credit history references misspelled.

In 1995, two sisters from the small town of Many, Louisiana, began to order merchandise from companies across the country. Soon truckloads of packages were being delivered. By the time Postal Inspectors and sheriff's deputies arrested them on June 7, 1997, both of their houses and a nearby storage facility were overflowing with fraudulently obtained merchandise. Along with using their home addresses and post office boxes in seven surrounding towns, the sisters created 364 fictitious name variations to conduct their mail order fraud scheme. Federal prosecution resulted in guilty pleas from both women and partial restitution later in the same year. Actual losses were estimated at more than $100,000.

- Credit history use of payment terms such as "unlimited" or "instant."
- Partial payment leading to credit extension.
- Overpayment requiring refund of excess over actual merchandise cost.

General Information

- Any incomplete, inconsistent or inaccurate information on the mail order form.
- Nearest relative listed as a professional (doctor, dentist, engineer, etc.), especially with office phone number.
- Misspelled words and strange abbreviations.
- Punctuation mistakes.
- Colons in date of birth.
- Commas after numbers in address or year.
- Dashes between names or nouns.

Handwriting

Recurring patterns in handwriting characteristics on orders from different individuals should be a cause for alert. Additional warning signs follow.

"Floating" Periods

- Above the writing line.
- After the signature on the signature line.
- After the date on the signature line.
- On both sides of the middle initial.
- Throughout the application.

Signature

- Scrawled or illegible.
- Written over as if correcting a mistake.
- Underscored, underlined and/or angled off signature line.
- Name misspelled or first and last names reversed in signature.

Prevention Techniques

- Start with a freshly scrubbed and current mailing list (no older than 90 days).
- Run all potential applications through a known fraud address database (in-house, etc.).
- Carefully review the solicitations in known high-risk areas.
- Review and correct customer mailing list.
- Append (retain) phone numbers in database.
- Create a mail order form that makes fraudulent application difficult. Form should require:
  - First and last name and middle initial.
  - Complete address (city, state, ZIP+4).
  - Home phone and daytime and business phone.
  - An "Orders subject to approval" statement.
  - Disclaimers.
  - Photo identification for high-value orders, if applicable.

Note: To update and correct a mailing list, companies may choose to contact a local service bureau. The Postal Service certifies address software vendors through the Coding Accuracy Support System (CASS). Direct marketing companies should contact their postal account manager or the National Customer Support Center at (800) 238-3150 ext. 4495 for details of CASS-certified software.

Telephone Orders

Warning Signs

Many of the same informational warning signs for order forms should raise red flags in the telephone order process. In addition, direct marketing telephone staff should be alert to:

- Hesitation in answering questions.
- Unfamiliarity with basic categories of information requested.
- Changes in personal or financial information during the call.

Prevention Techniques

- Use of an on-line CASS address matching software can help in identifying fraudulent addresses while you have the customer on the line.
- Use Automatic Number Identifier (ANI) to identify the number from which the person is calling.
- Use ANI to compare to known fraud databases.
- Cross-check ANI telephone number with address verification rules.
- Create a database of all dialed-in telephone numbers and run the ANI numbers against the database to identify multiple applications originating from the same telephone number. (Multiple use or nondisclosure of a single number could reflect cellular phone activity.)
- Run addresses against the USPS National Change of Address and Delivery Sequence Files and cross-check directories for non-matching exceptions.
- Evaluate application and solicitation file phone number mismatches.

On-Line Orders

Warning Signs

Most of the warning signs that apply to mail and telephone orders apply to orders received electronically. In addition, direct marketers need to exercise caution because of the possible insecure transactions made via the Internet. Customer information can be easily compromised and misused by on-line criminals, making it extremely difficult to verify the identity of the person placing the order.

Prevention Techniques

- Run all potential applications through a known fraud address database (in-house, etc.).
- Cross-check data (e.g., does the phone number match the address?).
- Conduct reasonableness of information check (e.g., does the annual salary match the profession?).
- Contact direct marketing associations and Internet service providers for tips on preventing on-line fraud schemes.

Check Fraud

Warning Signs

Check fraud affects every direct marketing company. Industry sources estimate that check fraud and counterfeiting result in losses between $10 billion and $14 billion each year. There are several types of check fraud, including forgery (either as signature or endorsement), counterfeit checks, altered checks (either payee or amount), check kiting between accounts, third-party bill paying services, demand drafts and identity assumption fraud.

The following warning signs can be helpful in identifying "bogus" checks:

- Lack of perforation on at least one edge of check. Although some legitimate checks without perforation are now produced with laser printers, lack of perforation often is the first signal of a phony check.
- Inconsistent routing and fractional routing numbers. False numbering techniques are used by forgers to delay the presentation of the item at the bank. These techniques include altering the routing/transit number in the magnetic ink character recognition (MICR) line.

Prevention Techniques

- Educate and train order processing representatives to recognize check fraud.
- Train staff to become familiar with the MICR line, fractional routing/transit (ABA) number, serial number, perforation, and the typeface used by the banking institution, so that irregularities can be flagged.
- Use alternative payment methods offered by the Federal Reserve Bank, which can significantly reduce check fraud risk. Local Federal Reserve Banks have a detailed booklet on check fraud available on request.

Patterns of Suspicious Account Activity

This information is uncovered through additional investigation subsequent to the receipt of the order. It is often the result of close monitoring of database information on customers' ordering practices.

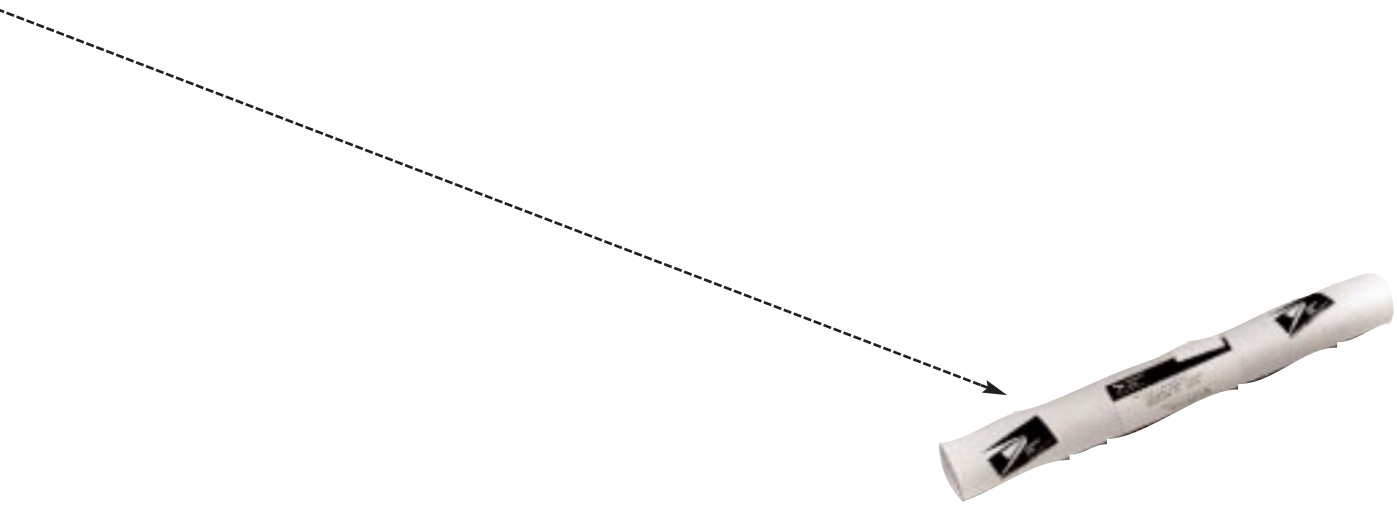
- Bad checks (NSF, closed account, etc.).
- Same-day or close-succession multiple orders before payment.
- Change of address immediately before or following merchandise order.
- High incidence of nonreceipt from same customer.
- Recently opened accounts with multiple orders/fast build-up of accounts.
- New customer with subsequent change of address.
- Orders for high-risk products (those with high resale value).
- Invalid Social Security number.
- Switch in merchandise.
- Change in ordering frequency and volume.
- Multiple new accounts.
- Recent delinquency.
- Credit balance/refund.
- Negative database match.
- Reactivating accounts.
- Certain merchandise return categories (return to sender or undeliverable).
- Continuous access and/or disconnects to integrated voice response or voice response unit.
- Nonpostal change of address attempts.
- Applications with requests for an authorized user who is not a spouse (should be outsorted for additional scrutiny).

Credit Reporting

Information included in a credit report may sometimes lead to a suspicion of fraud.

Warning Signs

- Recent creation of in-file date on top of the report.
- Fraud Alert or Fraud Victim Statement on the report.
- Address used previously for fraud.
- CMRA address.
- Post office box address.
- Home address actually institution address (e.g., hotel, mental institution, prison).
- Variation between address provided on application and most credible address on credit report.
- Address used multiple times by others.
- Address changed multiple times in a short period.
- Report indicates that Social Security number has not been issued.
- Social security number belongs to a deceased person (classified as retired by the Social Security Administration).
- Social security number being used by others.
- Social security number issue date inconsistent with applicant's age.
- Credit history inconsistent with applicant's age.
- Little or no variation in types of accounts (all credit cards; no mortgage, personal or auto loans).
- Substantial variance between age provided and age indicated on credit report.
- Abnormal amount of recent credit activity/inquiries.
- Applicant has substantial credit availability but requests more.
- Credit report reflects no activity, gaps or only recent activity on someone who claims to be 25 or older.
- Two or more names or variations in spelling of name.
- Applicant is an authorized user on most accounts on credit report or has two or more secured card accounts.
- Two or more recently opened accounts have "balanced amounts" that have exceeded their credit limits.
- Mismatch between employment provided and that listed on the credit report.
- Multiple employment listings with conflicting dates.
- Place of employment is fictitious.
- Authorized user has been added to a closed or dormant account.



EMPLOYEE, PLANT AND TRANSPORTATION SECURITY

Employee, plant and transportation security are vital to fraud and theft prevention efforts. A checklist of best security practices is available on page 31. This checklist may be helpful when reviewing internal security measures and those of subcontractors that handle mail, including presorters, consolidators and delivery firms.

Employee Security

- Develop a written company policy regarding employer/employee security.
- Develop a new employee orientation that includes a presentation of the company policy regarding employee security.
- Hold temporary employees to the same standards as regular employees.

Background Checks

- Require employee consent for background and credit checks in initial application for employment.
- Administer a drug screening as a condition of employment (refer to the state laws governing the issue).
- Verify previous employment, residency, education, and references for the past five years.
- Perform state and local criminal records checks in all states of residency/employment within the past five years.
- Obtain fingerprints of all employees.

Plant Security

- Designate one person to be responsible for all matters relating to physical security.
- Create a security control manual. Even if brief, it can document the level of security to be achieved and simplify the audit process monitoring safety compliance.
- Prohibit employees from taking personal bags into the work area.
- Utilize employee identification badges with photographs and maintain a duplicate.
- Use trusted, senior employees to process high-risk mail.
- Provide lockers away from the work floor and a place to secure personal belongings (coats, bags, cigarettes, etc.)
- Use pocketless and possibly color-coded aprons, if applicable.

- Use an electronic card access system to the facility and designate one entrance for employees. The card access system should provide different levels of security, depending on the work needs of the employees. In addition to limiting interior access, the system should also limit the times of day the employee will be admitted to the facility. Visitors should have limited and controlled access.
- Create a security staging area within an access controlled building to assure the safety of high-value merchandise. Ideally, an area that requires a second level of card access would be present.
- Shred or destroy material that contains customer account information before disposal.
- Install audible Underwriters Laboratory (UL) certified alarms on emergency doors. The system should be tested twice a year, and its maintenance documented. Hidden, manual alarms are also recommended for certain designated areas (e.g., public areas where high-value items are handled).
- Secure shipping and receiving docks from public access. This can be accomplished through the use of exterior fencing or detection devices.
- Focus closed-circuit television cameras on all areas in which theft might occur. This might include loading docks, staging areas, and employee exits. A system that uses color, a multiplexer, and an additional videocassette recorder for viewing tapes is recommended. Tapes should be maintained for at least 60 days.

Transportation Security

Transporting merchandise between the facilities of the mail order shipper, consolidator, and the Postal Service is a part of a mailing process that can be a risk. Security concerns include a lack of direct supervision, vehicle accidents, breakdowns, thefts by employees and robberies.

The following recommendations should serve as only a part of a well-planned and executed transport system for getting mail to the U.S. Postal Service for handling:

- Provide the transportation company with immediate means of notification in the event of an emergency.
- Maintain contact with the vehicle via a cellular phone or two-way radio.
- Have two employees in the same truck or employ a follow vehicle.
- Mark the transportation vehicle. There are various security philosophies regarding marked and unmarked vehicles. If unmarked vehicles are used, consideration should be given to marking the roof so that the vehicle can be located/identified by police authorities in the event of an emergency. In the alternative, a company-identified vehicle may be used.
- Use high-security locks on every vehicle. Test for wear and replace as needed. Higher levels of security can be reached through the use of tamper-evident security seals in addition to locks.
- Issue keys only to authorized individuals.
- Develop comprehensive contingency plans for vehicle breakdowns and delays and instruct all drivers as to how emergencies should be reported.
- Ensure that vehicle cargo areas are enclosed. Any windows should be secured with wire mesh.
- Use vehicles that restrict a driver's access to the cargo of the vehicle.
- Ensure that all drivers possess secure company identification. Changes in drivers should be immediately communicated to customers and suppliers to prohibit unauthorized access by employees and/or former employees.
- Off-load the vehicle as soon as possible after arrival at the destination facility.
- Never store mail in vehicles.

WORKING TOGETHER TO FIGHT MAIL ORDER FRAUD

The direct marketer is a partner with law enforcement in identifying and pursuing mail order fraud. Prompt and efficient action in pinpointing fraud or theft, maintaining accurate loss data and timely reporting of this information to the U.S. Postal Inspection Service are critical to the identification of suspects and subsequent successful civil and/or criminal prosecution.

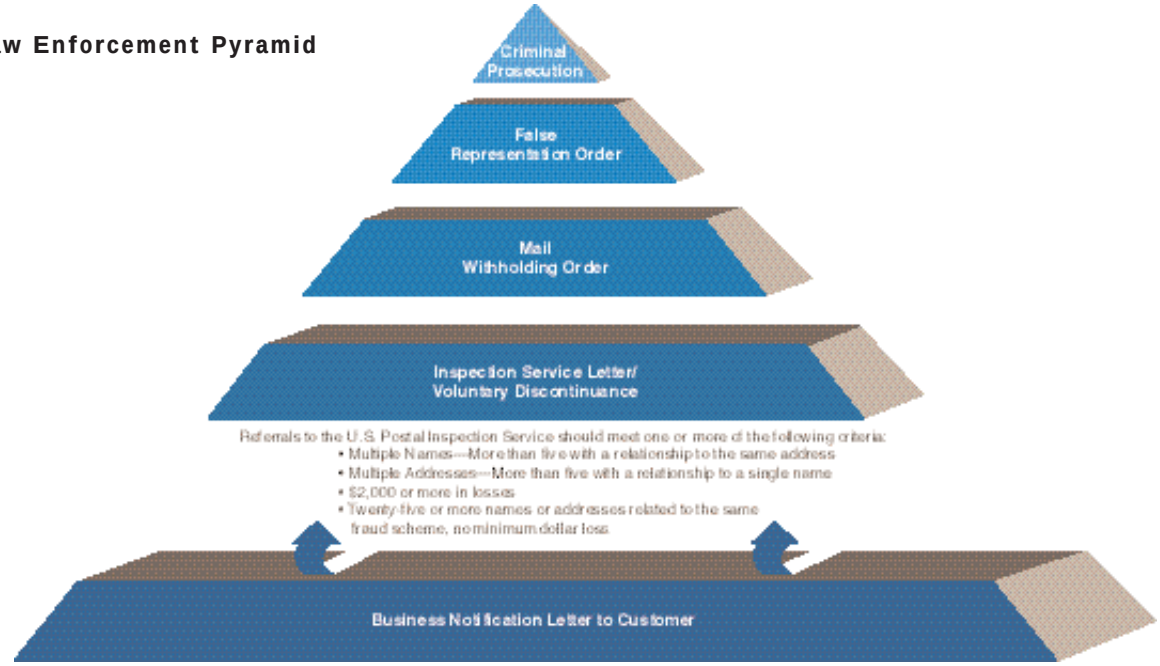
It remains the duty of direct marketers to protect their individual companies as fully as possible against loss. No prosecutor or judge is pleased to see public funds expended where fraud could have been easily prevented. But once mail fraud or theft is suspected and the necessary documentation is compiled, there are specific and reliable mechanisms for passing this information on and for cooperating with legal authorities in their investigation.

Law Enforcement Pyramid

The Law Enforcement Pyramid shown on the next page represents a succession of escalating options for dealing with suspected fraud and theft in the mail order industry. These include initial notification steps from the marketer to the problem customer, as well as the required method of reporting failure-to-pay fraud cases to the U.S. Postal Inspection Service. The pyramid progresses to criminal prosecution. Each situation is different, and is not automatically sent to advancing levels on the pyramid. Action on the pursuit of mail order fraud will be determined on a case-by-case basis.

The pyramid system is not designed to force-fit solutions to a problem. Before referring a case, direct marketing companies may want to check with their legal counsels to be sure that any procedure adopted complies with the law, and is not in conflict with company policies.

Law Enforcement Pyramid



The more detailed information a direct marketer can provide concerning a suspected fraud, the more likely it is that a remedy can be developed to address the situation. For assistance in pursuing actions described in the Law Enforcement Pyramid, contact the mail order coordinator at the nearest Postal Inspection Service Division Office. A current list of mail order coordinators is available from the Office of the Chief Postal Inspector.

Following are the steps and forms necessary to report mail theft and fraud, as well as the follow-through procedures used by legal authorities. Please note that only the Business Notification Letter and the Postal Inspection Service Referral Form are to be filled out by the direct marketing company. Other forms, included here as examples of legal follow-through, are strictly for the use of legal authorities in support of their investigation and prosecution activities.

Business Notification Letter

When a direct marketing company identifies possible fraud, the company directly contacts the individual to give notification that current or future orders cannot be filled without further clarification. This step is critical in documenting the company's initial effort to resolve the problem and/or discontinue further loss. One company, after initiating its own notification letter, reported a 50% reduction in fraud losses. A sample letter is included on page 34. This is a suggested letter only; each company should structure a letter tailored to its own legal requirements and specific needs.

Referral to Postal Inspection Service

If the problem persists and the loss/fraud meets established referral criteria, then the company may move to the next level of the pyramid by completing the Postal Inspection Service Referral Form (sample on page 32) and returning it to the nearest Postal Inspection Service Division Office, attention mail order coordinator. Information on the suspected fraud is now advanced to law enforcement attention. It is at this common

referral point that large-scale fraud schemes are often revealed, with several companies sustaining losses to the same offender at the same addresses. This becomes a factor when evaluating what remedy to bring to bear on a particular problem, and highlights the importance of each company's responsible reporting of theft and loss through the mail.

Referral Criteria

Referrals to the Postal Inspection Service should cite one or more of the following criteria within six months of the referral submission.

- Use of multiple names — more than five names with a relationship to the same address.
- Use of multiple addresses — more than five addresses with a relationship to a single name.
- $2,000 or more in losses.
- Twenty-five or more names or addresses related to the same fraud scheme, no minimum dollar loss.

On the basis of the referral(s) received, investigating Postal Inspectors may then apply the tools and remedies identified in the next levels of the pyramid. While the direct marketer may be called on for assistance with additional information or cooperation in prosecution, from this point on the pursuit of suspected fraud or theft is primarily in the hands of law enforcement authorities.

A CLOSER LOOK

In California, a manager at a small direct marketing company made note of an unusual number of items shipped to private mail boxes at CMRAs. At the same time, her data processing staff reported an increase in the number of usually reliable customers listed as late for payment on orders shipped. Within minutes it was clear that these events were related, and that the losses incurred were significant. The fulfillment manager reported the evidence of fraud to the company's chief operating officer. They were eager to pursue the crime but uncertain of the best course of action. The company contacted the Postal Inspection Service and worked with Postal Inspectors to identify and apprehend the violator before additional losses were incurred.

U.S. Postal Inspection Service Actions

Voluntary Discontinuance Letter and Statement of Voluntary Discontinuance

With the Voluntary Discontinuance Letter, the Postal Inspection Service attempts to place the suspected fraud perpetrator on notice of possible civil and criminal actions if the activity continues. Accompanying the letter is a Statement of Voluntary Discontinuance, which requests that the customer cease the activity, sign the statement and submit it by return mail to the Postal Inspection Service. If the agreement is subsequently violated, Postal Inspectors may take action to withhold the individual's mail, pending additional administrative proceedings. This statement also provides documentation for stronger sanctions. Samples of the Postal Inspection Service Voluntary Discontinuance Letter and the Statement of Voluntary Discontinuance are included on pages 35 and 36.

Withhold All Mail (WAM) Orders

When there is strong indication that a person is using a fictitious, false or assumed name to escape identification when conducting a mail fraud scheme, Postal Inspectors can apply Title 39, U.S. Code, Section 3003, and obtain a WAM Order. The individual must come forward and furnish proof of identity and of his or her right to receive the mail. If the individual cannot satisfy these requirements, an administrative law judge may permit the Postal Service to return all mail to the sender.

False Representation Orders

Through the Postal Service judicial officer, the Postal Service is empowered under Title 39, U.S. Code, Section 3005, to issue False Representation Orders (FROs) and Cease and Desist Orders. These orders require the fraud perpetrator to stop engaging in the cited schemes. The FRO directs that all mail be returned to the sender. The violator of Cease and Desist Orders may be subject to civil penalties under Title 39, U.S. Code, Section 3012.

Title 39, U.S. Code, Section 3007, allows the Postal Service to seek a Temporary Restraining Order and a Preliminary Injunction from a U.S. district court judge to detain mail until administrative proceedings conclude. In addition, a U.S. district court judge may hold a hearing on alleged fraudulent activity and issue a restraining order or injunction enjoining the operation pursuant to Title 18, U.S. Code, Section 1345.

By convincing the court to withhold mail while a case is argued, Postal Inspectors have been successful in limiting the extent of victimization. Action taken under these statutes does not preclude criminal charges against the same target. Moreover, Postal Inspection Service investigations may result in restitution to the victims.

Criminal Prosecution

At the top of the pyramid is criminal prosecution. All criminal activity involving use of the U.S. Mail with intent to defraud can be prosecuted under the Mail Fraud Statute, Title 18, U.S. Code, Section 1341. The Mail Fraud Statute is the oldest consumer protection law in the United States and is one of the most effective prosecution tools in fighting white collar and organized crime. Criminal prosecution may be considered when less severe remedies have not been successful in terminating the fraudulent activity or when the fraud operation or losses have become extensive.

Note: Prosecutive guidelines vary from district to district and state to state. Therefore, it is important for direct marketers to furnish documents and witnesses as necessary to support criminal prosecutions. Failure to supply information in a timely manner can damage future referrals to prosecutors.

MAILING WITH SUCCESS

The best products and the most thoughtfully prepared advertising materials will not succeed without adequate preparation. This section provides some of the basic information needed to plan a mailing and work with the U.S. Postal Service in ensuring that both the mailing and merchandise reach customers. Customer claims of nonreceipt can have several causes, including addressing, packaging and processing problems. To avoid problems, all mailpieces must meet specified Postal Service guidelines.

Following are guidelines, definitions, and steps in the process that will ensure the best use of the Postal Service and the highest level of customer satisfaction. The same mail management techniques that have made direct mail advertising a cost-effective marketing channel can also be applied to billing statements and merchandise.

Getting It Right

The U.S. Postal Service is committed to working with businesses to provide a variety of fast, reliable, and economical ways to send printed material, merchandise, and correspondence. Direct marketing companies should consult the *Domestic Mail Manual (DMM)* for the most current information on Postal Service rules, regulations, services, postage, and reduced prices.

Local post offices can provide information on most of these topics. You can call 1-800-222-1811 for additional direction. To order a current copy of the *DMM* complete the order form on page 47 or visit the Postal Service website (www.usps.gov).

Delivery Address

The delivery address must be legible, complete and appear on the side of the mailpiece that bears the postage. Guidelines for addressing a mailpiece are in Postal Service Publication 28, *Postal Addressing Standards*, which can be obtained by contacting the National Customer Support Center at (800) 238-3150, or by downloading it from the Postal Service website (www.usps.gov).

A Postal Service mailpiece design analyst can review a sample mailpiece before it is printed and mailed to ensure that it is compatible with mail processing equipment. Direct marketing companies can contact a mailpiece design analyst through their postal account manager.

Packaging

There are many reasons why a mailpiece may not get delivered to its intended addressee in a timely manner. One reason is that packaging may lose its integrity before leaving the mailer's distribution center(s) or consolidators operations, or while in the Postal Service mailstream. When packaging opens during processing, the mailpiece is sent to the rewrap operation causing, at a minimum, delivery delays. In a worst case scenario, the contents become separated from the packaging and the article becomes "undeliverable" or a nonreceipt item.

Sortation

Mailings sent at discounted bulk rates require special preparation, including presorting. Presorting is the process of arranging mail so that mailpieces going to the same area (as determined by ZIP Code and, in some cases, route number) are grouped together, allowing mail to bypass certain handling stages during processing. Bypassing stages in mail processing keeps mailings more intact and reduces processing errors, untimely delivery or possible loss.

For more details on presorting and mail preparation, contact a postal account manager or consult the *DMM*.

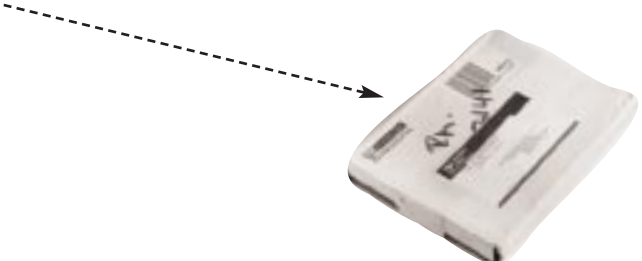
Forwarding and Return of Undeliverable Mail

Every attempt is made to deliver all mail as addressed to any authorized customer mail receptacle or post office box. Mail undeliverable as addressed will be further processed if there is a return address and an ancillary service endorsement is used. No matter what endorsement is printed on the mailpiece, if no return address is present, the mailpiece will be treated as undeliverable and must be forwarded to one of three mail recovery centers. Mailers should establish a proactive relationship with such centers through their account managers. The early detection and correction of addressing and packaging problems can avoid consumer complaints of nonreceipt, and reduce company costs associated with replacement shipments.

Ancillary Service Endorsement

Ancillary service endorsements are used by mailers to request an addressee's new address, and to provide the Postal Service with instructions on how to handle undeliverable pieces. Endorsements consist of one keyword — Address, Forwarding, Return, or Change — followed by the two words Service Requested.

For more information, contact the National Customer Support Center at (800) 238-3150.



CHECKLIST AND SAMPLES

By working together, the U.S. Postal Inspection Service and the direct marketing industry can effectively fight mail order fraud and nonreceipt. The following pages offer a security checklist and letter samples that will assist with joint fraud efforts and explore the Law Enforcement Pyramid described on pages 24 through 27.

Security Checklist

The following checklist should be used to help ensure employee, plant and transportation security. Any "No" answer should include an explanation as to why that particular security measure is not being followed. The checklist may also be helpful when reviewing the security measures of your subcontractors such as presorters, consolidators and delivery firms.

	YES	NO
Employee		
• Are background investigations being conducted?		
• Is there a new employee orientation that includes company security policies?		
• Are temporary employees held to the same standards as regular employees?		
Plant		
• Are personal items kept away from the work area?		
• Are work areas restricted to employees on duty only?		
• Are picture identification cards issued to employees and are they worn at all times?		
• Are break/smoking areas away from the work area?		
• Are work areas arranged to eliminate employees working out of sight or alone for prolonged periods?		
• Are supervisors' desks/work stations out in the open where everyone can see them?		
• Is there an individual responsible for security?		
• Does the security person make unscheduled tours of work areas?		
• Is the closed-circuit television system in place and operational for the employee entrance, parking lots, loading docks, supply rooms, stairwells and other points of risk?		
• Is an access control system in place and operational?		
• Is there a designated employee entrance/exit for exclusive use?		
• Is the alarm system in place and operational for burglaries and robberies?		
• Is there a security manual?		
• Are security policies and procedures prominently posted at employee entrances, in break areas, and on bulletin boards?		
• Is the perimeter of the facility properly secured?		
• Is the locker room separate from the work area?		
Transportation		
• Are all vehicles equipped with cellular phones or two-way radios?		
• Are all vehicles equipped with locks and/or tamper-evident security seals?		
• Has a contingency plan been developed to include vehicle repair or replacement?		
• Are the transportation vehicles marked so that they can be identified by police authorities in the event of an emergency?		
• Are vehicle keys issued only to authorized personnel?		
• Is the cargo area restricted from access by the driver?		
• Are all drivers in possession of company identification?		
• Are vehicles off-loaded as soon as possible after arrival at the destination facility?		

Postal Inspection Service Referral Form

Company Name: _____

Contact Person: _____

Telephone Number: _____

Type of Complaint: _____

Various Names: _____ Number Involved: _____

Various Addresses: _____ Number Involved: _____

Primary Address Involved: _____

_____

_____

Is Address Still Active? Yes ❒ No ❒

Date Merchandise Was Last Shipped: _____/_____/_____ Date of Last Contact: _____/_____/_____

Total Loss: $ _____

Was Merchandise Shipped via U.S. Postal Service? Yes ❒ No ❒

TYPE OF MERCHANDISE:

Books/Magazines ❒ General Merchandise ❒ Tapes/CDs ❒

Other (please specify): _____

Business Notification Letter Sent? Yes ❒ No ❒

If yes, date of letter: _____/_____/_____

If yes, did customer respond? Yes ❒ No ❒

Amount of Loss Sustained Since Letter Was Sent: $ _____

This form can be copied, completed and sent to the nearest Postal Inspection Service Field Division Office, attention mail order coordinator. A list of Postal Inspection Service Field Division Offices is on the following page. Attach any supporting documentation to the Referral Form.

POSTAL INSPECTION SERVICE FIELD DIVISION OFFICES

Atlanta Division
P.O. Box 16489
Atlanta, GA 30321-0489
(404) 608-4500

Cincinnati Division
895 Central Ave., Suite 400
Cincinnati, OH 45202-5748
(513) 684-8000

Gulf Coast Division
P.O. Box 1276
Houston, TX 77251-1276
(713) 238-4400

Memphis Division
P.O. Box 3180
Memphis, TN 38173-0180
(901) 576-2077

Miami Division
3400 Lakeside Dr., 6th Fl.
Miramar, FL 33027-3242
(954) 436-7200

Michiana Division
P.O. Box 330119
Detroit, MI 48232-6119
(313) 226-8184

Mid-Atlantic Division
P.O. Box 3000
Charlotte, NC 28228-3000
(704) 329-9120

Midwest Division
1106 Walnut St.
St. Louis, MO 63199-2201
(314) 539-9300

New York Metro Division
P.O. Box 555
New York, NY 10116-0555
(212) 330-3844

Newark Division
P.O. Box 509
Newark, NJ 07101-0509
(973) 693-5400

Northeast Division
425 Summer St., 7th Fl.
Boston, MA 02210-1736
(617) 464-8000

Northern California Division
P.O. Box 882528
San Francisco, CA 94188-2528
(415) 778-5800

Northern Illinois Division
433 W. Harrison St., Room 50190
Chicago, IL 60669-2201
(312) 983-7900

Northwest Division
P.O. Box 400
Seattle, WA 98111-4000
(206) 442-6300

Philadelphia Metro Division
P.O. Box 7500
Philadelphia, PA 19101-9000
(215) 895-8450

Rocky Mountain Division
1745 Stout St., Suite 900
Denver, CO 80202-3034
(303) 313-5320

San Juan Division
P.O. Box 363667
San Juan, PR 00936-3667
(787) 749-7600

Southern California Division
P.O. Box 2000
Pasadena, CA 91102-2000
(626) 405-1200

Southwest Division
P.O. Box 162929
Ft. Worth, TX 76161-2929
(817) 317-3400

St. Paul Division
P.O. Box 64558
St. Paul, MN 55164-0558
(612) 293-3200

Tampa Division
P.O. Box 22526
Tampa, FL 33622-2526
(813) 281-5200

Washington Metro Division
P.O. Box 96096
Washington, DC 20066-6096
(202) 636-2300

Western Allegheny Division
1001 California Ave., Room 2101
Pittsburgh, PA 15290-9000
(412) 359-7900

Business Notification Letter

(Date)

(Customer name and address)

Dear (customer):

Thank you for your recent communication. We have a problem with the address you provided to us. The following items need further clarification:

____ Multiple outstanding orders have been received for this address.
____ Multiple names have been used for this address.
____ Multiple changes of address have been received for this address.
____ Nonreceipt of merchandise.
____ Other

We are aware that there are people who take advantage of mail order and publishing companies by submitting fraudulent orders for merchandise. In an effort to protect our customers' interests, we routinely review our records to detect fraudulent activity. Of course, it is a violation of the Mail Fraud and Postal False Representations Statutes (Title 18, U.S. Code, Section 1341; Title 39, U.S. Code, Section 3005) to use the U.S. Mail to order merchandise with the intent not to pay for it. Violations of these statutes may be referred to the U.S. Postal Inspection Service for investigation.

We need your help. Please call us at (phone #) with any information that could help clear up this problem.

Sincerely,

(company representative signature)

(Note: This letter is intended only as an example of the initial Business Notification Letter. Different or additional letters may be sent to the customer, depending on the particular problem or company policy. It is suggested that this letter be sent by First-Class certified mail with return receipt requested so it can be tracked internally.)

Voluntary Discontinuance Letter

[U.S. Postal Inspection Service letterhead]

(Date)

Dear Postal Customer:

This office is investigating a possible violation of federal law with which you may be associated involving failure to pay for ordered merchandise.

We sometimes find that individuals are unaware that they may have violated the mail fraud statutes; at other times, we find that individuals have intentionally defrauded businesses. When we find a violation, our objective is to stop the use of the mail to conduct the fraudulent activity. Continued activity could result in further legal action.

Many companies offer attractive incentives to order their products or services through the mail. These incentives motivate customers to order their products; however, they also require consumers to fulfill certain obligations. Failure to pay for ordered merchandise is illegal under the Mail Fraud Statute, Title 18, Section 1341 of the U.S. Code; and under the Postal False Representation Law, Title 39, Section 3005 of the U.S. Code.

When submitting an order for a product or service, a person represents to the seller that he or she intends to comply with the terms of the offer, including subsequent required purchases or payments. When multiple names or variations of a street address are used, an individual is falsely representing to the company that each order is from an actual person residing in that household. That individual is also causing something of value, the product, to be sent through the mail based on one or more false representations.

Once a person has been notified that certain conduct is illegal, continuing the activity could provide legally sufficient evidence that the illegal activity was intentional.

If you feel that you may have unknowingly been involved in the activity described above, please cease any further action that may result in further legal action. By signing and returning the attached Voluntary Discontinuance Form, you are not admitting to any wrongdoing; rather, you are simply agreeing to discontinue the practice.

If you agree to stop the activity, write "REFUSED" across the face of any unopened mail you receive connected to the activity, mark a line through your name and address, and return it to the post office for return to sender.

Our primary concern is to see this activity stopped. Enclosed for your convenience is a preaddressed envelope that requires no postage. Your cooperation would be appreciated.

U.S. Postal Inspector

Statement of Voluntary Discontinuance

PLACE:

DATE:

STATEMENT OF VOLUNTARY DISCONTINUANCE

I, (Name) _____, have been informed by representatives of the U.S. Postal Inspection Service that the failure to pay for merchandise ordered through the mail may constitute a violation of Title 39, U.S. Code, Section 3003, Mail Bearing a Fictitious Name or Address; Title 39, U.S. Code, Section 3005, False Representations; and/or Title 18, U.S. Code, Section 1341, Frauds and Swindles.

I have decided to voluntarily discontinue and abandon all use of the mail in connection with any failure-to-pay activity that I may have committed unknowingly.

I am keeping one copy of this statement and am returning the other copy to the Postal Inspection Service.

_____

(Sign your name)

_____

(Print your name)

_____

(Your telephone number, including area code)

_____

(Print your address)

GLOSSARY OF USEFUL TERMS

Presented here are useful terms pertaining to the Postal Service and its services and to mail fraud and nonreceipt. No attempt is made to provide a complete lexicon for all of direct marketing, a field in which rapid development has been accompanied by new technology, changes in meaning, and a rapid turnover in terminology.

A

Account Takeover Fraud
Access and/or manipulation of existing account information by an unauthorized individual(s) for the purpose of committing fraud.

Address Change Service (ACS)
An automated process that provides change-of-address information to participating mailers who maintain computerized mailing lists. The information is captured in the Computerized Forwarding System II units and sent to mailers electronically to eliminate manual input of change information into their mailing systems.

Address Correction Service
An ancillary service that provides a mailer with the forwarding address of the addressee (if the addressee filed a change-of-address order with the USPS) or the reason for nondelivery. It is available alone or in combination with forwarding and return service.

Address Information System Products
USPS addressing products and services used to obtain the correct USPS ZIP Code, ZIP+4 or carrier route number for mailing list addresses. These include computerized products such as the City State File, 5-Digit ZIP Code File, Line-of-Travel (LOT) information, Z4CHANGE File, ZIPMOVE File, Carrier Route Information System, and ZIP+4 tapes. They also include printed ZIP Code and ZIP+4 directories and microfiche products. For more information contact the National Customer Support Center at (800) 238-3150.

Address Service Requested (ASR)
If mail is undeliverable, the endorsement "Address Service Requested" in the upper left corner of the mailpiece will provide the mailer with the forwarding address of people who have filed a change-of-address order, or will indicate a reason for nondelivery (such as "no such address," "unknown at this address," "forwarding time expired," etc.). The charge for this service varies, depending on the class of mail and the weight of the mailpiece.

Adverse Action Notice
A notification required by the Equal Credit Opportunity Act (ECOA) and Fair Credit

Reporting Act (FCRA) that informs a credit applicant that the creditor has declined the application. This notice must be sent by the creditor within 30 days of having received the completed application.

Alternate Mailing System (AMS)
A procedure that provides for accepting permit imprint mail to ensure proper postage payment and mail preparation without verification by weight.

Ancillary Service
Forwarding, return, or address correction service included within a mail class. Depending on the mail class, these services are performed at a charge or at no additional charge if and when the service is actually rendered.

Annoyance Order Fraud
Occurs when a disgruntled individual orders merchandise for another individual without his or her authorization. This scheme results in the victim receiving unwanted merchandise and subsequent payment requests from numerous direct marketing companies. Annoyance order fraud is a form of harassment and can sometimes ruin a victim's credit rating.

Apartment (Numbers)
Designation by letters or numerals (or both) of dwelling units in multi-family buildings. "Occupant" mailers can reach each apartment by its code, but mail addressed by name only is often difficult to deliver.

B

Back End
All activities performed by the direct marketer that occur once a promotion is launched. Back-end performance relates to purchase behavior over a given period of time by respondents.

Barcode (BC)
A series of vertical bars and half bars that represent correct ZIP Code information for the delivery address on a mailpiece. The barcode facilitates automated processing by barcode reader equipment. Each numeric digit is represented by a combination of two full bars and three half bars. A complete barcode contains two full bars framing the code; the 5, 9, or 11 digits containing ZIP Code information; and a final correction digit that allows the machine to check its reading of the number.

Bill to/Ship to Fraud
A fraud scheme that involves shipping mail order merchandise to an address different from the billing address.

Bound Printed Matter (BPM)
Standard Mail (B) weighing at least 1 pound, but not more than 10 pounds, that consists of permanently bound sheets of which at least 90% are printed with advertising, directory, or editorial matter (or a combination of such matter).

Bulk Business Mail (BBM)
Periodicals and Standard Mail (formerly third- and fourth-class mail) submitted in bulk to business mail entry units or other designated facilities. The term includes samples, ordinary papers, and circulars.

Bulk Mail Center (BMC)
A highly mechanized mail processing plant that is part of the National Bulk Mail System. This facility distributes Standard Mail (A) and Periodicals in bulk form and Standard Mail (B) in both piece and bulk form.

Business Mail Entry Unit (BMEU)
The area of a postal facility where a mailer presents for acceptance bulk mail or presorted mail. It includes dedicated platform space, office space, and a staging area on the workroom floor. (Formerly called bulk mail acceptance unit, platform acceptance unit, or weigher's station.)

Business Reply Mail (BRM)
Specially printed postcards, envelopes, cartons, and labels that may be mailed without postage prepayment. Postage and fees are collected when the mail is delivered back to the original sender. This domestic service enables authorized mailers to receive First-Class Mail, without prepaid postage, back from customers by paying the postage and fee on receipt of the mailpieces.

C

Carrier Route Code
The alphanumeric code provided on a mailing label to identify a given carrier route. These codes are updated every six months by the Postal Service, which furnishes a CRIS tape (carrier route information system) to be used for carrier route coding and sorting.

Carrier Route Information System (CRIS)
The official city delivery scheme that lists all city and noncity delivery post offices, which is available to mailers in a standardized format. It contains schemes for city routes, rural routes, highway contract routes, post office box sections, and general delivery units. The data are formatted by ZIP Code, street name, and street number range. Delivery statistics (possible deliveries) for each carrier route are also included in the file. (See also Coding Accuracy Support System.)

Carrier Route Presort (Carrier Rate Postage)
Mail that the mailer arranges by carrier route to qualify for discount postage rates. The mail requires no primary or secondary distribution. The term is a general descriptor of the available rates for this type of preparation, including Enhanced Carrier Route Standard Mail, automation carrier route First-Class Mail, carrier route Periodicals, and carrier route Bound Printed Matter. Except for automation rates, this mail usually does not bear a barcode.

Casing
The way the postal carrier, in office, sorts mail into a "case" with pigeonholes for his or her route in Walk-Order, then "pulls" the mail in the order in which he or she delivers the route.

Certification
The Postal Service periodically tests the accuracy of the commercial software that uses postal files for processing. Address matching software used in ZIP+4 processing must be CASS-certified annually. On a voluntary basis, vendors may PAVE-certify postal presort software, and may certify the accuracy of the barcode print image.

Change of Address Fraud
Occurs when a false change of address is submitted by a criminal to forward a victim's mail to a delivery address under the control of the criminal. The false change of address is sent to either the direct marketing company or to the Postal Service. Often the victim does not realize anything is amiss until he or she fails to receive mail for a period of time. Meanwhile, the criminal receives both the mail and mail order merchandise.

Change of Address Processing
A means to match known movers to a list prior to mailing to provide correct new addresses for such movers. (See National Change of Address.)

Check Fraud
Nonpayment for merchandise using bad checks. Examples of bad checks include stolen or counterfeit checks and nonsufficient funds checks.

Claims Paid Fraud
Occurs when merchandise has been shipped to a customer and received, but payment has not been received from the customer. However, the customer claims that he or she has already paid for the merchandise.

Claims Returned Fraud
Occurs when a customer claims that he or she returned the merchandise to the direct marketing company but the company does not receive the merchandise.

Cleaning
A term used to describe the updating of a list to remove "undeliverable as addressed" (or aging) data from a file.

Cluster Box Unit
A centralized unit of individually locked compartments for the delivery of mailpieces.

Coding Accuracy Support System (CASS)
A service offered to mailers, service bureaus, and software vendors that improves the accuracy of delivery point barcodes, ZIP+4 codes, 5-digit ZIP Codes, and carrier route information on mailpieces. CASS provides a common platform to measure the quality of address matching software and useful diagnostics to correct software problems. (See also Carrier Route Information System.)

Commercial Mail Receiving Agency (CMRA)
A private business that acts as the mail-receiving agent for specific clients. The business must be registered with the post office responsible for delivery to the CMRA. These private mail box addresses are often used to facilitate financial and mail order fraud.

Cooperative
Any form of direct-response advertising involving offers from more than one mailer. Includes billing stuffers, package inserts, "cardvertiser" decks, split panels, or pages in self-standing stuffers, "ridealongs", and all forms of "marriage mail."

Courtesy Reply Mail (CRM)
A preaddressed return envelope or postcard that business mailers provide to a customer for returning a remittance, order, or response. The customer pays the postage. In many cases, the envelope is also prebarcoded.

Credit Application Fraud
Occurs when someone obtains a financial transaction instrument through falsification of information provided to the issuer of the application with the intent to defraud the credit issuer.

D

"Deadbeat" List
A list of "bad pays" or poor risks.

Deceased Customer Fraud
Occurs when merchandise is ordered in the name of a deceased person and, when received, payment is not made. When the direct marketing company inquires about payment, they are told that the original customer has died.

Delivery Sequence File (DSF)
The DSF, compiled by the Postal Service, is a comprehensive database of every one of the 120 million addresses to which the Postal Service delivers. The DSF serves as a tool to improve mailing list selections and to provide walk sequencing of mail files. DSF processing will confirm the accuracy of mailing lists, identify address errors, and provide information about the address. DSF processing is performed by commercial vendors under license by the Postal Service. Outside lists compared to the DSF by one of a handful of licensees can make a substantial contribution to reducing wasteful mailings.

Demand Draft
A financial document that resembles a personal check but carries no signature. In place of a signature, it has a notice that the account holder has given permission to have money withdrawn from his or her checking account to pay for goods or services.

Destination Delivery Unit (DDU) Rate
A discount/rate available to Periodicals and Standard Mail (A) carrier route mail that is properly prepared and entered by the mailer at the delivery unit that serves the address on the mail.

Domestic Mail Manual (DMM)
A directive that contains the basic Postal Service standards for domestic mail services; a description of and requirements for each mail class special service and ancillary service and conditions governing their uses and standards for rate eligibility and mail preparation. It is one of six Postal Service policy manuals.

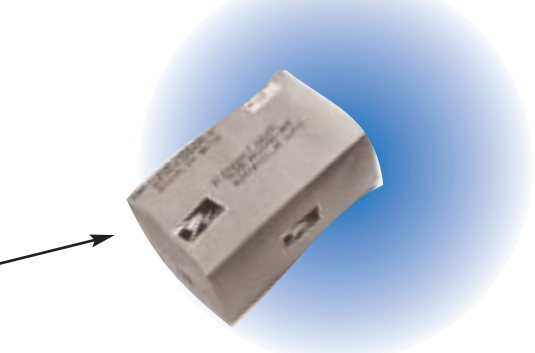
Drop Date
The date a mailing is scheduled to be delivered to the Postal Service.

Drop Shipment
A mailing transported by the mailer or a private (nonpostal) carrier, from the point of production to a postal facility located closer to the destination. Express Mail and Priority Mail™ drop shipment service can be used instead of a private carrier.

Dwelling Type
Consumers live in one of two kinds of dwelling units, single-family units or multiple-unit dwellings. Almost 19% of the American population lives in multiple-unit dwellings, the great majority in high-rise buildings.

E

11-Digit Bar Coded Addressing
All barcoded mail now includes 11 digits: the 9-digit ZIP Code, plus the last 2 digits of the local address. Now there is also a check digit, something the 9-digit ZIP Code never provided.



F

False Credit Application Fraud
A type of fraud that is very common in the mail order industry. This involves obtaining a credit line or establishing an account based on false information supplied to the company by the criminal.

False Damage Claim Fraud
This occurs when a customer claims that the merchandise was received in a damaged condition and requests a replacement when, in fact, the merchandise was not damaged. In this way, the customer is able to receive two or more of the same product for the price of one.

First-Class Mail (FCM)
A mail class that includes all matter wholly or partly in handwriting or typewriting, all correspondence, all bills and some statements of account, and all matter sealed or otherwise closed against inspection. First-Class Mail comprises three subclasses: Post and Postal Cards, Letters and Sealed Parcels, and Priority Mail. Any mailable matter may be sent as First-Class Mail. First-Class Mail is a USPS trademark.

Fraud
The intent to obtain merchandise or something of value without payment; typically involves deception or misrepresentation of material facts. (See Mail Fraud.)

Fulfillment
The actions taken after printed pieces and mailing list data are delivered to the mailing service plant to get a mailing into the mailstream; also refers to the physical handling of an order, an information request, or a premium or a refund.

I

Identity Theft and Account Takeover
A type of mail order fraud scheme also called "True Name" fraud. Identity theft fraud occurs when an individual steals another's personal information such as a date of birth or Social Security number and uses the information to open new accounts without that person's knowledge. Merchandise is ordered using the new identity and sent to an address controlled by the criminal. The victim only discovers the fraud after the mail order company notices unusual activity and inquires about the new account. Identity theft and account takeovers often involve use of false changes of address submitted to the mail order company or the U.S. Postal Service.

Indicia (Meter Indicia)
An imprinted designation on a mailpiece that denotes postage payment (e.g., a permit imprint in place of a postage stamp or a meter stamp).

L

Lettershop
A lettershop handles all details of printing and mailing letters and stuffers while a mailing house essentially handles the preparation and the mailing of bulk quantities of mail.

M

Mail Count
An enumeration (in pieces or pounds) of the amount of mail sorted or handled.

Mail Date
The date selected for delivery of a mailing to the U.S. Postal Service. Working backward from this date, mailers can calculate time needed for creation, purchasing, printing, assembling, and fulfillment.

Mailer
The organization that enters mail in the postal mailstream. For Standard Mail (A) this includes more than 750,000 establishments with permits; that is almost 1 of every 10 establishments in America. The mailing house is also sometimes referred to by this term.

Mail Fraud
The intentional obtaining of merchandise or something of value without payment and typically involves deception or misrepresentation of material facts. A mail fraud violation occurs when the U.S. Mail is an integral part of a fraud scheme. The Mail Fraud Statute (a felony) is contained in Title 18 of the U.S. Code, Section 1341. This statute is the oldest consumer protection law in the United States.

Mailing House
A direct mail service establishment which, among other services for the mailer, will affix labels, sort, bag, and deliver the mail in qualified ZIP Code strings to the Postal Service for certification.

Mail Monitoring
A means to determine how long individual pieces of mail take to reach their destinations; also utilized to verify content and ascertain any unauthorized use.

Mail Preference Service
A well-advertised program of the DMA providing a means to consumers to remove their names from a large number of mailing lists.

Mail Recovery Center (MRC)
A postal facility designated only to receive and attempt to return undeliverable and unforwardable mail of obvious value. Unpaid mail without a return address is also sent to one of these facilities.

Mail Stop Order
An order issued by the USPS judicial officer that directs the post office of delivery to return to the sender any mail responding to a false representation or lottery scheme.

Manifest Mailing System (MMS)
A postage payment system that enables the USPS to accept and verify permit imprint mailings that contain nonidentical-weight and/or nonidentical-rate pieces of the same mail class (except Periodicals) and same mail processing category. These pieces are prepared by the mailer according to certain standards.

Marriage Mail
A form of co-op in which the offers of two or more mailers are combined in the same folder or envelope for delivery to the same household or establishment.

Multiple Names/Addresses Fraud
A type of fraud that occurs when a customer intentionally deceives the direct marketing company by using various names and addresses to receive merchandise and fails to pay for the orders. This type of fraud often uses commercial mail receiving agency (CMRA) addresses for receipt of shipped merchandise.

N

Name Removal
Names are removed prior to mailing if they match the DMA Mail Preference File (see Mail Preference Service), if requested by the customer, if marked "Do Not Mail," if known to be a nondeliverable address, or if matching against the Delivery Sequence File (DSF) so indicates.

National Change of Address (NCOA)
An address correction service provided to mailers by the USPS through its licensees. All change-of-address data submitted by relocating customers are transmitted daily from Computerized Forwarding System (CFS) sites to the USPS National Customer Support Center (NCSC) at Memphis, TN. The NCSC consolidates the data, places them on computer tape, and then standardizes the addresses against the ZIP+4 Code database. The licensees match computerized mailing lists with change-of-address data, and NCOA provides current standardized and ZIP+4 coded addresses for all residential and business movers before the mail enters the mailstream. (See also Address Change Service.)

National Customer Support Center (NCSC)
A USPS organization that provides information, services, and products (e.g., zone charts, directories, software programs, testing of ZIP+4 code or delivery point code address matching software) that are designed to improve the quality of addressing for mailings that qualify for certain rates. The NCSC can be reached at (800) 238-3150 or www.usps.gov.

Nonreceipt
A customer claims that (a) merchandise was not received; (b) merchandise was ordered, received, and then returned to the mail order company, which did not receive the return; or (c) merchandise was neither ordered nor received, although he or she is billed. Nonreceipts may occur as a result of damage in handling or theft during shipment.

O

Overpay Refund/Bad Check Fraud
Occurs when a customer sends a check for payment of merchandise in excess of the amount owed. The direct marketing company issues a refund to the customer for the excess amount and then later finds that the original customer check is not honored. Often, in these cases, the customer may receive both the merchandise and the refund check.

P

PAVE
PAVE (presort accuracy validation and evaluation) is a process that certifies presorting software. A list of PAVE-certified software vendors is available on the U.S. Postal Service website (www.usps.gov).

Periodicals
A mail class (formerly called second-class mail) consisting of magazines, newspapers, or other publications formed of printed sheets that are issued at least four times a year at regular, specified intervals (frequency) from a known office of publication. Periodicals usually must have a list of subscribers and/or requesters, as appropriate.

Permit
An authorization, typically a mailing permit, to mail using an indicia containing specific information regarding postage payment.

Plant-Verified Drop Shipment (PVDS)
A procedure that enables origin verification and postage payment for shipments transported by the mailer from the mailer's plant to destination post offices for Postal Service acceptance as mail. PVDS is typically used for mailings for which a destination entry discount is claimed.

Postage Statement
Documentation provided by a mailer to the Postal Service reporting the volume of mail being presented and the postage payable or affixed, and certifying that the mail meets applicable eligibility standards for the rate claimed.

Presort
Sorting mail using Postal Service standards prior to mailing.

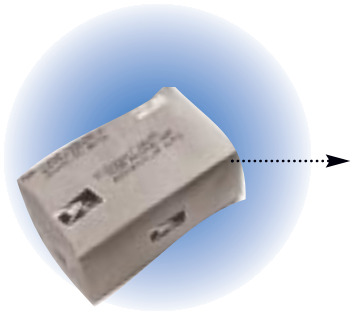
PS Form 3602
This is the Statement of Mailing that must be provided by the mailer of any bulk mailing. PS Form 3602 identifies the class of mail, level of sortation, postage rate, number of pieces, and postage due. It provides certification by the Postal Service.

R

Rates and Classification Service Center (RCSC)
A field office of Postal Service headquarters that provides guidance to postal employees and customers on mail classification, postage rates, mail preparation standards, and postage payment programs.

Return Postage Guaranteed
An optional Postal Service delivery service. By printing this message in the upper left corner of a mailpiece, the mailer requests the return of any undeliverable mailpieces. The mailer pays return postage plus a return fee for each piece.

Return Receipt for Merchandise
A special service that provides the sender with a mailing receipt and a return receipt. A delivery record is kept at the office of address. It does not include insurance coverage and does not provide for restricted delivery.



S

Scams
A type of blatant fraud where the offer is a rip-off, often directed to vulnerable, older or unsophisticated citizens.

Ship to Address
Delivery address. Businesses usually include both a "Bill to" address (for purchasing or accounting) and a "Ship to" (delivery) address on order forms.

Standard Mail
A mail class consisting of mailable matter that is not mailed as First-Class Mail or entered as Periodicals. Standard Mail includes matter formerly classified as third-class and as fourth-class mail. Though combined in Standard Mail, matter from each former class remains subject to separate and specific classification, eligibility, and preparation standards. Matter formerly classified as third-class mail is referred to as Standard Mail (A); matter formerly classified as fourth-class mail is referred to as Standard Mail (B). The unmodified term Standard Mail applies to both former third-class mail and former fourth-class mail.

Standard Mail (A)
Standard Mail matter that weighs less than 16 ounces. It comprises the subclasses of Regular Standard Mail, Nonprofit Standard Mail, Enhanced Carrier Route Standard Mail, Nonprofit Enhanced Carrier Route Standard Mail, and Single-Piece Standard Mail. These subclasses include circulars, printed matter, pamphlets, catalogs, newsletters, direct mail, and merchandise. Standard Mail (A) may be sent at presorted rates and at automation rates.

Standard Mail (B)
Usually Standard Mail matter that weighs 16 ounces or more. It comprises four subclasses: Bound Printed Matter, Library Mail, Parcel Post, and Special Standard Mail.

T

True Name Fraud
A type of mail order fraud scheme often called "Identity Theft and Account Takeover" fraud. True name fraud occurs when an individual steals another's personal information such as a date of birth or Social Security number and uses the information to open new accounts without that person's knowledge. Merchandise is ordered using the new identity and sent to an address controlled by the criminal. The victim only discovers the fraud after the mail order company notices unusual activity and inquires about the new account. Identity theft and account takeovers often involve use of false changes of address submitted to the mail order company or the U.S. Postal Service.

U

Undeliverable as Addressed (UAA)
Mail that the USPS cannot deliver as addressed and must forward to the addressee, return to the sender, or send to a mail recovery center (depending on treatment authorized for that mail class).

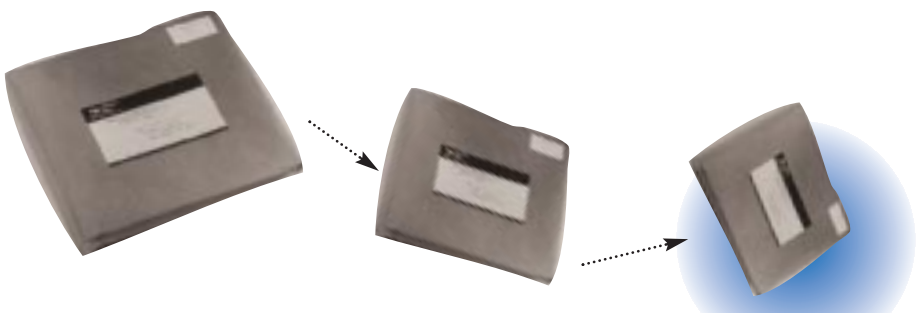
W

Walk-Order
Lists sorted to individual carrier routes in the precise order in which each route is walked for delivery of the mail. Almost all occupant or resident mail is in Walk-Order sequence. Any list matched against the DSF (Delivery Sequence File) is automatically sorted into Walk-Order sequence.

Z

ZIP Code
The 5-digit numeric code, established in 1963, of which the first 3 digits identify the delivery area of a sectional center facility or a major-city post office serving the delivery address area. The next 2 (the fourth and fifth) digits identify the delivery area of an associate post office, post office branch, or post office station. All post offices are assigned at least one unique 5-digit code. ZIP Code is a USPS trademark.

ZIP+4
The 9-digit numeric code, established in 1981, is comprised of two parts: (a) The initial code — the first 5 digits that identify the sectional center facility and delivery area associated with the address, followed by a hyphen; and (b) the 4-digit expanded code: the first 2 additional digits designate the sector, and the last 2 digits designate the segment. ZIP+4 is a USPS trademark.



Order Form for the Domestic Mail Manual (DMM)

SUPERINTENDENT OF DOCUMENTS ORDER FORM — DOMESTIC MAIL MANUAL

Phone Orders: **(202) 512-1800** Order Processing CODE #5573
Fax Orders: **(202) 512-2233**

❒ Yes, please send me _____ subscription(s) to Domestic Mail Manual (DMM) at $30 for one year ($37.50 foreign). I understand my subscription will begin with the most recent issue published.

The total cost of my order is $_____. Price includes regular shipping and handling and is subject to change.

Mailing Address

_____
Company or Personal Name

_____
Additional Address/Attention Line

_____
Street Address

_____
City, State, ZIP Code

_____
Area Code and Telephone (day)

Payment Method

❒ Check payable to Superintendent of Documents

❒ GPO Deposit Account ☐☐☐☐☐☐☐–☐

❒ MasterCard/Visa

Card Number_____

Expiration Date_____

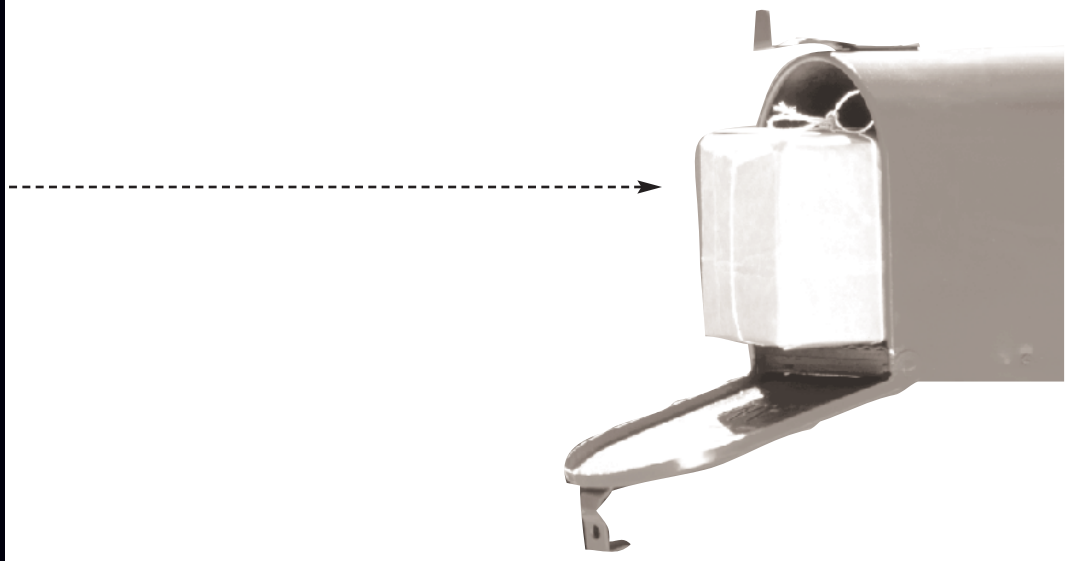
_____
Cardholder's Signature

For privacy protection, check the box below:
❒ Do not make my name available to other mailers.

Mail to: **Superintendent of Documents**
Mail Stop SSOM
732 N. Capitol St. NW
Washington, DC 20402-9375

Customers may order *The Postal Explorer* (on disk) for $20 by faxing (901) 681-4542. *The Postal Explorer* includes the *DMM* (Issue 53), *International Mail Manual (IMM* Issue 19), updated domestic and international rate calculators, and several new publications. The Government Printing Office will mail each subscriber only one renewal notice. To change your address, fax (202) 512-2168 or send new mailing label and new address to:

SUPERINTENDENT OF DOCUMENTS
MAIL STOP SSOM
732 N CAPITOL ST NW
WASHINGTON DC 20402-9375



ACKNOWLEDGEMENTS

The Mail Order Task Force wishes to thank the following companies who participated in the task force and sponsored this guide.

Advertising Mail Marketing Association
Artistic Greetings
Bear Creek Operations
BMG Direct
Book of the Month Club
Brylane, L.P.
BTE
Caremark, Inc.
Chadwick's of Boston
Clark-American
Columbia House
Cosmetique
Cowles Creative Publishers
CTC Distribution Services, L.L.C.
Current, Inc.
Deluxe Check Printers
Direct Marketing Association, Inc.
Doubleday Direct
Eastern Collection Corp.
Experian
Fingerhut Corporation
First of Omaha
First USA Paymentech
Fleming Co. Inc.
Foster & Gallagher
Gateway 2000
Gevalia Kaffe
Greybarn, Ltd.
Grolier Direct Marketing
Hanover Direct
Heritage House
Home Shopping Network
Insight
J. Crew Group
Lenox
Lillian Vernon
L. L. Bean
Marketing Data, Inc.
MasterCard
National Geographic Society
National Wholesale Company
Neodata
Newport News, Inc.
Nationwide Fraud Investigations
Publishers Clearing House
QVC
Reader's Digest Association
RMX Logistics
Rodale Press
Sears, Roebuck & Co.
Southern Progress
The Bradford Exchange
The Credit Index
The Franklin Mint
The Sportmans Guide
Time Life Inc.
TransUnion Corp.
Trans Union National Center
U.S. Mint
U.S. Sales
Val-Pak
Value Vision
Warren, Gorham & Lamont