GENERAL RESOURCE GUIDE FOR CREDIT CARD FRAUD AND IDENTITY THEFT

When receiving inquiries from the public regarding and identity, bank, credit card or other type of fraud, it is recommended that the possible victims follow these suggestions:

- If the fraud or identity theft is such that it does not meet the federal guidelines in your district, the victim should be referred to the proper local law enforcement agency to file a report

- The victim should be advised to contact any affected credit card issuer by telephone and advise them of the situation and request the following action be taken:

    1. The victim should request replacement cards with new account numbers.
    2. The old account should be processed as "account closed at consumer's request" for credit record purposes.
    3. Ask that a password be used prior to any purchases on the new account.
    4. The victim can also ask that all of their accounts be flagged, and that a victim's statement be added. This ensures that financial institutions contact the victim to verify their credit applications.

    Advise the victim to follow-up the telephone call with a letter to the credit card issuer, summarizing their requests.

- The victim should be instructed to also contact all three credit bureaus and report the compromise. The credit bureaus can be contacted at:

Equifax	800/525-6285	www.equifax.com
Experian	888/397-3742	www.experian.com
Trans Union	800/680-7289	www.tuc.com

- The victim should order copies of credit reports so that they can review them to ensure that no additional fraudulent accounts have been opened in their name. This should be done every three months for at least one year.

Other steps that can be taken by the victim include:

- The victim can also call 888/567-8688 to opt out of receiving pre-screened credit card offers. All three credit bureaus will honor this one request.

- The victim should contact the Social Security Administration's Office of the Inspector General, at 800/269-0271, if a Social Security Number has been used fraudulently.

- File a complaint with the FTC (The Federal Trade Commission is the federal clearinghouse for complaints by victims of identity theft. All victims should report the incident to them.) by calling: 1/877/IDTHEFT, or by writing to, Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, or online at www.consumer.gov/idtheft.

Some additional tips for safeguarding personal information:

- Explain the Social Security number is the key to credit and banking related accounts. People should only provide their Social Security number if it is absolutely necessary, and only to trusted parties.

- Try to reduce the number of credit cards in use.

- Cancel unused credit card accounts.

- If a fraudulent charge appears on an account, call the Consumer Credit Counseling Service 800/388/2227 for help in clearing false claims from credit reports.

- Destroy (shred) pre-approved credit applications, credit card receipts, bills and any other financial information that is unneeded. Throwing then in the trash is not sufficient unless the applications are first made unintelligible.

- Unwanted JUNK mail can be reduced by contacting Direct Marketing Association's Mail Preference Service, P.O. Box 9008, Farmingdale, NY 11735-9008. Request that your name and home address be removed from all mailing lists.

- Unwanted telemarketing solicitations, can be reduced by the Direct Marketing Association's Telephone Preference Service, P.O. Box 9014, Farmingdale, NY 11735-9014. Request that your name and telephone number be removed from all telemarketing lists.

- To remove your email from many marketing lists, thus reducing some of the spammed email you receive, visit www.e-mps.org.

- Dial *67 prior to making 800, 888, and 900 number telephone calls. In most cases this will prevent your name, address and phone number from being captured by the company you're calling.

- If ordering on-line, insure that the company you're dealing with is not selling or trading your personal information. Remember, most businesses keep the information that is provided to them on-line, in some type of database. These databases can be sold or accessed by others without your knowledge or consent.