If the Red Flags Compliance Officer discovers or suspects that there has been an incident of identity theft, the following letter should be sent from the Red Flags Compliance Officer to the patient (or customer) whose identity was stolen. A copy of the FTC Identity Theft Complaint and Affidavit should be attached.

[Date]

Via Certified Mail, Return Receipt Requested
Article No. _____
[Patient or Customer Name and Address]

Re: Possible Identity Theft

Dear _____:

It appears that there may have been suspicious activity on your account maintained by _____ County on *[date]*. *[Explain the factual situation of the compromised information, how it happened, what information was disclosed and what actions have been taken to remedy the situation]*. This incident has been reported to the _____ County Sheriff's Office, which can be reached at _____. We have also placed an alert on your account in an effort to prevent further misuse of your identity.

Identity theft has become a serious problem that can cause financial harm. It may take a long time to correct. It is imperative that you take swift action. Medical identity theft can lead to inappropriate medical care when incorrect information is included in a patient's medical record. We request your assistance in ensuring that our records about you are correct.

If you find that you are a victim of identity theft, please take the following steps as soon as possible:

1. Fill out the attached FTC Identity Theft Complaint and Affidavit.
2. Contact the fraud departments of each of the three major credit bureaus and report the theft. Ask that a "fraud alert" be placed on your file and that no new credit be granted without your approval. Below is the name and phone number of each of the major credit bureaus:

Equifax: 1.800.525.6285

Experian: 1.888.397.3742

Trans Union: 1.800.680.7289

3. For any accounts that have been fraudulently accessed or opened, contact the security department of the appropriate creditor or financial institution. You may want to consider closing these accounts. You should consider new passwords that are not your mother's maiden name or Social Security number on any new accounts you open.

4. Get a copy of the law enforcement report number or a copy of the report in case the bank, credit card company or others need proof of the crime later.

5. Call the Federal Trade Commission's ID Theft Clearinghouse toll-free at 1.877.ID.THEFT (1.877.438.4338) to report the theft. Counselors will take your complaint and advise you on how to deal with the credit-related problems that could result from ID theft. The Identity Theft Hotline and the ID Theft Website (www.ftc.gov/idtheft) give you one place to report the theft to the federal government and receive helpful information. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves and stop them.

If it appears that you have been a victim of medical identity theft, then you should take the following steps:

1. Ask to review your medical records at the office of each of your medical provider's offices. If there is any incorrect information, you should advise the office of the appropriate corrections.

2. Carefully monitor explanations of benefits (EOBs) or other information that you receive from your health insurer to determine if any other person has used your identity to obtain health care. If you receive an EOB or medical bill for a service that you did not receive, immediately contact your health insurance company and health care provider who furnished the services.

3. Notify other health care providers that your identifying information is being used in a fraudulent manner.

If there is anything that _____ County can do to assist you, please call me at _____.

Sincerely,

_____ County Red Flags Compliance Officer