State of Illinois
Department of Human Services

IDENTITY ALERT FORM

To be completed by DHS personnel when the identity of a customer is in doubt.

Form completed by: _____ Date: _____

Title: _____ Division/Office/Bureau: _____

Location, e.g. Woodlawn FCRC, Elgin Mental Health Center: _____

Person presented to DHS using the following information.

Name: _____ Phone: _____

Address: _____

Social Security Number: _____ Birthdate: _____

Case I.D. Number: _____ Date of presentation for services: _____

Insurance information presented including Medicaid, Medicare, other government programs, or private insurance:

_____

Policy Number: _____

Reason the person came to DHS for services: _____

What proof of identity was given to you? For example a photo I.D., pay stub, utility bill?

Explain the circumstances of this alert. For example, what made you suspect that this could be a fraudulent request. List any witness(es) here:

Do you believe this person was attempting to use another customer's benefits or identity? If so, explain why. If known, document which customer might be a victim of I.D. theft, or misappropriation of benefits, and their case I.D. number.

ATTACH A COPY OF THE RELEVANT PHOTO I.D. OR OTHER INFORMATION GIVEN TO YOU AS PROOF OF IDENTITY. FORWARD THE COMPLETED FORM TO THE LOCAL PRIVACY OFFICER AND LOCAL ADMINISTRATOR.

IDENTITY ALERT FORM

Guidance for using the Identity Alert Form

It is part of our job as DHS employees to guard customers' confidential, medical, and financial information from identity theft, misappropriation, or intermingling. The Identity Alert form should be used in conjunction with DHS Administrative Directive 01.01.01.180: Identity Theft and Misidentification of Customer and Employee Information. Please refer to it, or ask your supervisor if you have questions

The purpose of this Form is to identify circumstances in which:

- someone may be attempting to use another person's identity
- someone may be attempting to use another person's benefits
- someone may try to establish eligibility for services using fake or stolen identification
- someone may have had their identity or SSN stolen
- someone may have had someone else's personal or health information mixed in with their own information

These circumstances can occur in the following ways:

- Suspicious documents: Has a new customer given you identification documents that look altered or forged? Is the photograph or physical description on the ID inconsistent with what the customer looks like? Did the customer give you other documentation inconsistent with what he or she has told you, for example, an inconsistent date of birth or a chronic medical condition not mentioned elsewhere? Under the Red Flags Rule and Administrative Directive, you may need to ask for additional information.

- Suspicious personally identifying information:. A customer gives you information that does not match what you've learned from other sources. For example, if the customer gives you a home address, birth date, or SSN that doesn't match information on file or from the insurer, it could be a fraudulent request for services.

- Suspicious activities: Is mail returned repeatedly as undeliverable, even though the customer still shows up for appointments? Does a customer complain about receiving a bill for a service he or she didn't get? Is there a inconsistency between a physical examination or medical history reported by the customer and the treatment records? These may all be red flags for identity theft.

- Notices from victims of identity theft, law enforcement authorities, insurers, or others suggesting possible identity theft. Have you received word about identity theft about a customer from another source? If so, let your supervisor know about it. Cooperation is the key when it comes to assisting our customers prevent identity theft.