USDA United States Department of Agriculture
Food and Nutrition Service

Introduction to Biometric Identification Technology: Capabilities and Applications to the Food Stamp Program

Office of Research and Analysis **December 1999**

Summary

In its continuing efforts to safeguard the integrity of the Food Stamp Program (FSP), the U.S. Department of Agriculture's Food and Nutrition Service (FNS) initiated this study of the use of biometric identification technologies in the FSP. As a method of reliably verifying the identity of applicants, biometric identification has the potential to reduce the vulnerability of the Food Stamp Program to duplicate participation, which has also been referred to as "double dipping."

Biometric identification technology provides automated methods to identify a person based on physical characteristics – such as fingerprints, hand shape, and characteristics of the eyes and face – as well as behavioral characteristics – including signatures and voice patterns. Although used in law enforcement and defense for several years, it has recently been used in civilian applications, such as the FSP and other assistance programs. This technology has the potential to identify individuals who attempt to apply for benefits on more than one case, or who attempt to obtain benefits belonging to someone else.

This report presents an overview of biometric identification technology with particular attention to its potential use to improve the integrity of the FSP. It briefly describes some of the major technologies, summarizes their capabilities, gives examples of applications, and discusses issues that should be considered in evaluating biometric identification technology. It pays particular attention to applications of the technology to the FSP, or to other welfare programs. Although it describes several specific biometric identification technologies, it focuses on finger imaging, which has been the primary technology used in social service programs. A companion report describes the efforts of nine States that have incorporated or plan to incorporate biometric technology in their social service programs, and discusses the cost and effectiveness of these programs, as well as the reactions to them by the client population.

Description of Biometric Technology

Biometric identification technology uses automated methods to recognize the identity or verify the claimed identity of an individual based on physical or behavioral characteristics. A biometric identification device is capable of measuring individual biometric information, comparing the resulting measurement with one or more stored biometric reference templates, deciding whether they match sufficiently to indicate that they represent the same person, and indicating whether or not a recognition or verification of identity has been achieved.

One of the most common methods of biometric identification is based on the analysis of finger images. Most automated finger image identification technology uses a process analogous to that used by a human fingerprint analyst. Finger images are processed by the software to identify the location and orientation of minutiae, which include points where fingerprint ridges diverge and points where ridges stop. The minutiae of a live image are then compared to one or more stored images. If they are sufficiently similar, then a match is declared. The steps in processing a finger image include capture of the image, image processing, feature detection, and matching.

Initial applications of biometric identification technology were for police or military organizations. More recently, biometric technology has been applied to a wider variety of civilian applications. The technology provides authentication for computer system access, eases entry into the country for frequent international travelers, replaces passwords in automated teller

machines (ATMs), and verifies the time workers spend on the job. Applications differ in several ways; the specific characteristics of an application can affect the performance of the technology and its vulnerability to certain attempts at fraud.

Applications to the FSP

There are two ways to use biometric identification technology to reduce FSP fraud: when an individual enrolls for benefits and when the benefits are redeemed at a local grocery store. The goal of biometric identification technology at enrollment is to eliminate individuals who apply for duplicate benefits using more than one identity by detecting or deterring those who apply for duplicate benefits. The goal of biometric technology at disbursement is to reduce trafficking or other unlawful uses of benefits by those who are not entitled to receive them.

System Performance and Effectiveness Issues

A biometric method used at the time of application to reduce fraud in the FSP must be quick, accurate, resistant to fraud, and acceptable to clients. In addition, the technology will not be effective if it is vulnerable to attempts to change the appearance of a finger image in order to avoid detection of a duplicate applicant. Analysis of existing data suggests that finger-imaging systems are capable of detecting more than 95% of attempts to obtain duplicate benefits while incorrectly indicating fraud in fewer than 1% of legitimate applicants. System error rates can be improved by using human minutiae analysts to examine candidate matches or performing periodic unfiltered searches of the entire finger-image data base.

The performance of a biometric identification system is affected by policy decisions. For systems used at the time of enrollment, the policies regarding exemptions from biometric requirements might affect the likelihood of catching fraudulent attempts to obtain duplicate benefits. Though exemptions are required for those who are missing fingers or who cannot provide an image with sufficient quality for identification, exemptions for other reasons, such as individuals who are certified outside of the office or who have a religious objections to finger imaging, depend on agency policy.