E·C·I
Economic Crime Institute of Utica College

LexisNexis™

Using Identity Authentication and Eligibility Assessment to Mitigate the Risk of Improper Payments

A Joint Project of the Economic Crime Institute of Utica College and LexisNexis, a Division of Reed Elsevier Inc.

January 28, 2005

Dr. Gary R. Gordon
Professor of Economic Crime Programs
Executive Director of the Economic Crime Institute
Utica College

Mr. Norman A. Willox, Jr.
Chief Officer for Privacy, Industry, and Regulatory Affairs
LexisNexis, a Division of Reed Elsevier Inc.

Foreword

In a continuing effort to provide cutting edge research, Utica College's Economic Crime Institute has partnered with LexisNexis to conduct this research study on improper payments. This white paper is a continuation of three earlier works on identity fraud sponsored by LexisNexis. Dr. Gary R. Gordon and Norman Willox were the principal authors of *Identity Fraud: A National and Global Threat*, released in October 2003. The white paper is available at http://www.ecii.edu/pub_whitepapers.html. Norman Willox, Jr. and Thomas Regan authored *Identity Fraud: Providing a Solution* in March 2002. It can be retrieved at http://www.lexisnexis.com/about/whitepaper/IdentityFraud.pdf. An earlier work by Willox and Regan entitled, *Identity Fraud: Searching for a Solution*, was released in October 2001. The URL is http://www.shepards.com/risksolutions/IdentityFraud.pdf.

About the Authors

Dr. Gary R. Gordon is the principal author of this study. He is Professor of Economic Crime Programs at Utica College and the Executive Director of the Economic Crime Institute.

Mr. Norman A. Willox, Jr., Chief Officer, Privacy, Industry, and Regulatory Affairs, LexisNexis, provided directional and expert support. Dan Duncan, CEO, Austin Logistics, was a significant contributor to Section 3: Applying Risk Assessment Methodology to Improper Payment Management.

Economic Crime Institute of Utica College

Utica College, a world leader in economic crime prevention education, provides fully accredited bachelor's and master's degree programs in economic crime Investigation and management (http://www.economiccrimedegrees.com/). In conjunction with key personnel at the Department of Homeland Security, Utica College has established a four course graduate risk assessment certificate that is offered inside DHS for its staff only.

The Economic Crime Institute of Utica College drives leading-edge thinking on economic crime issues faced by business and government, through educational programs, policy guidance, research, and solutions. The Institute, founded in 1988, is a forum for the exchange of ideas, solutions, and technology for managing the risk of economic crime and fraud (www.ecii.edu).

LexisNexis

In the U.S., LexisNexis (www.lexisnexis.com) offers an extensive range of products and customized tools that address job-specific and organization-wide information needs, driving productivity and confident decision-making. For 30 years, LexisNexis has been an information solution provider. Through its risk management flagship products, Accurint®, Banko®, PeopleWise®, and RiskWise®, LexisNexis products help to authenticate identity, locate people and assets, enable commerce, conduct background screening, and support national security initiatives. Customers include government agencies, top law firms, and major companies in the fields of national security, financial services, collection and recovery, insurance, mortgage, telecommunications, e-commerce and retail.

Abstract

Fraud, waste, and abuse losses are major challenges for entitlement programs. Because these programs constitute a large part of the government's annual budget, even a small percentage of fraud, waste, and abuse results in staggering losses.

The "Improper Payments Information Act of 2002" (PL 107-300) requires agencies to assess the risks of making improper payments. This includes a statistically valid determination of the amount of improper payments in their programs, identification of the root causes, a plan to reduce improper payments in those programs that are deemed vulnerable, and an annual report to identify the risks and reduction methods.

This paper addresses strategies for mitigating risk of improper payments through identity authentication and eligibility assessment. While this paper focuses solely on applying risk assessment strategies, it is anticipated that future white papers will focus on internal controls (solutions), and the recovery process.

Anecdotal and pilot test data are presented to illustrate the identity challenges that facilitate improper payments. Proven risk assessment and management methods are presented to demonstrate how they can mitigate eligibility and entitlement weaknesses. An information based identity authentication system solution is recommended to combat improper payments where identity fraud/theft, at both the enrollment and post award stages, is a root cause.

There is considerable concern that individuals who do not meet the eligibility criteria are receiving entitlement benefits. This may be due to several reasons, including misrepresentation of financial information, identity fraud and theft, account takeover, and misallocation of funds. For example, data mismanagement results in misallocations of funds, which creates opportunities for fraud and abuse that otherwise would not have existed. This paper suggests a methodology for improving on eligibility assessment in the enrollment phase and in post award analysis.

Table of Contents

Part I
Introduction

Fraud, waste, and abuse losses are major challenges for entitlement programs. Because these programs compose a large part of the government's annual budget, even a small percentage of fraud, waste, and abuse results in staggering losses.

In addressing this problem, it is important to explore the nexus of identity fraud/theft and improper payments. As Gordon et. al. state in their 2003 white paper, *Identity Fraud: A National and Global Threat*, identity fraud/theft is a well-documented problem. Given the vulnerability of identity authentication systems, it is not surprising that individuals and organized groups have used fictitious and assumed identities to facilitate improper payments. Some of the anecdotal cases reveal that this is not a new phenomenon.

The link between identity and eligibility criteria is an important part of the nexus of identity fraud/theft and improper payments. However, the extent to which it is a root cause of improper payments is not known. Two pilot studies discussed in this paper provide evidence that identity fraud/theft presents a significant opportunity to commit fraud, resulting in improper payments. Applying identity authentication systems, when determining eligibility and reviewing existing recipients' files for information anomalies, is a promising avenue for mitigating this problem.

Size and Scope

The size of the improper payment problem is well documented. Recent OMB and GAO reports indicate colossal losses; however, most of the data is reported in the aggregate.

OMB reported the top ten areas of improper payment in FY 2002:

- Medicare, fee-for-service – $13.3 billion
- Earned Income Tax Credit – $9.2 billion
- Housing Subsidy Programs – $3.3 billion
- Supplemental Security Income – $2.6 billion
- Unemployment Insurance – $2.2 billion
- Food Stamps – $1.3 billion
- Old age and survivors insurance – $875 million

Definitions

Improper Payments: any payment that should not have been made or that was made in an incorrect amount under statutory, contractual, administrative, or other legally applicable requirement. Improper amounts are overpayments and under payments (including inappropriate denials of payment or service). An improper payment includes any payment that was made to an ineligible recipient or for an ineligible service. Improper payments are also duplicate payments, payments for services not received, late payment interest not earned, and payments that do not take credit for appropriate discounts. (OMB Circular A-11)

Identity Fraud: the use of false identifiers, documents, or an assumed identity in the commission of a crime. This could include misrepresenting one's identity by changing specific personal identifiers (Gordon and Willox, 2003).

Authentication: methods used to determine if the person claiming the identity is really that person or the entity is really the claimed entity.

Information Based Identity Authentication: an independent assessment of what a person and/or entity represents about his or its identity, based on analysis of available information (Gordon and Willox, 2003).

Personal Identifiers: permanent and temporary attributes associated with an individual or an entity.

Eligibility Assessment: validation, verification, and authentication methods used to determine whether the applicant meets the criteria for an entitlement through independent sources of information. Unlike a background investigation that reviews many facets of an individual, this approach is targeted to the scope of criteria that must be met to receive an entitlement.

Enrollment Phase: process of adding a person or an entity to a system for the purpose of granting a credential or providing a benefit. As this phase acts as the gatekeeper of the system, due diligence in the form of an assessment of criteria and authentication ("proofing") of identity is critical.

- Disability Insurance – $825 million
- Medicare cost reports – $493 million
- Student Assistance Pell Grants – $336 million (Gerow 2004)

Fiscal Year 2003 Performance and Accountability Reports Provide Limited Information on Govenmentwide Improper Payments, a GAO study, reports estimates of more than $35 billion in improper payments based on the reporting of 31 of the 46 agency programs estimated losses.

Unfortunately, there is no statistical data on the causes of improper payments. For example, it would be interesting to know how frequently identity problems result in the facilitation of improper payments or how weaknesses in the controls for determining eligibility result in improper payments. This information would address one of the reporting requirements of the Improper Payments Information Act: "…a discussion of the causes of the erroneous (improper) payments identified, actions taken to correct causes, and results of the actions taken to address those causes." (Office of Management and Budget, 2002a.)

The Improper Payment Information Act of 2002

The Improper Payment Information Act of 2002 requires agencies to comply with a four step process to reduce improper payments: "(1) identify susceptible programs for significant improper payments; (2) identify the amounts of the improper payments in the susceptible programs; (3) implement a plan to reduce the improper payments; and (4) report the estimates."

OMB Memorandum (M-03-13) provides additional clarification and guidance for complying with the act.

"These particular steps are as follows:

1. Compile and inventory all payments/outlays.
2. Conduct risk assessments.
   - Identify those programs the agency believes have an error rate of at least 2.5% and an error amount in excess of $10 million.
3. Conduct statistical analyses.
   - Take a sample of payments in those programs identified in Step 2 above.
   - Track those payments through an audit/ verification process to assess error.
   - Use information found in the sample to extrapolate an error rate and amount for the program as a whole.
4. Develop corrective action plans.
   - For those programs in Step 3 above that are found to have in excess of $10 million in improper payments, develop a plan for eliminating those payments.
5. Develop a baseline and improvement targets.
6. Report results annually in the Performance and Accountability Report (PAR)." (Springer, L. , 2004)

♦♦♦

Part II
Identity Problems and Improper Payments

This section begins with anecdotal reports of improper payment cases that were facilitated using fictitious or assumed identities. While these cases illustrate the connection between identity and improper payments, they do not answer the question of size and scope. The second part of this section reviews two pilot studies that help to shed light on the potential size and seriousness of the problem.

Anecdotal Data

In his June 15, 2004 Congressional Testimony before the Committee on Ways and Means Subcommittee on Social Security, Acting Inspector General for the Social Security Administration, Patrick P. O'Carroll, Jr, stated that increasing incidences of identity theft involving Social Security numbers is an "epidemic that must be brought under control." In addition, O'Carroll noted that, "criminals use identity theft to defraud Federal agencies and programs of millions of dollars" (O'Carroll, 2004).

There are numerous cases where improper payments from government entitlement programs have been facilitated by identity fraud or theft. A few are noted here to illustrate the nexus of identity fraud/theft and improper payments.

Citing the Inspector General of the Department of Education, Charles Gerow noted several examples of such abuse in his Testimony on Improper Payments before the Subcommittee on Government Efficiency and Financial Management on April 15, 2004. They include a case in which a supposed student of a community college in Arizona used prison inmate identities in a scheme to receive student aid. He was "successful" in his endeavors, netting more than $300,000 in student aid payments. In another case, a financial aid director was able to receive more than $14,000 in loans from the Federal Family Education Loan Program by using a fictitious name (Gerow, 2004).

O'Carroll cited an example in his June 15, 2004 testimony in which a Florida resident received over $79,000 in survivors benefits for herself and three fictitious children. She was able to obtain an identification card from North Carolina by assuming the identity of someone she once knew. With the identification card and fraudulent birth certificates, she applied for and was granted Social Security Numbers for two fictitious children. She furthered her scheme by inventing an ex-husband and father for the non-existent children, using the name of a person who was known to be dead. She then applied for and received survivor benefits for herself and the supposed children. The third fictitious child had been created previously, as part of a similar crime through which she received survivor benefits.

In the June 28, 2004 issue of EYE on OIG, it was reported that a landlord assumed the identity of a deceased tenant and for 19 years received the money that the deceased woman would have received as the beneficiary of an SSA retirement insurance policy.

In the Office of Inspector General Department of Veterans Affairs Semi-Annual Report to Congress (October 1, 2003-March 31, 2004) a case involving identity theft was included. A non-veteran used a matching Social Security card and veterans identification card from a legitimate veteran to obtain medical services from four Veterans Affairs Medical Centers.

While not focused on specific cases, two other mentions of this connection were found in the literature search. A case illustration from a 2001 GAO study reports on a risk assessment approach and findings from Centrelink, an Australian organization. "The risk assessment identifies 'fictitious or assumed identities' and 'undeclared or understated income' as the risk categories that pose the greatest exposure of improper payments after existing controls have been considered" (GAO-02-69G). In a recent industry white paper, the authors state, "Identity fraud, whether conducted by individuals or businesses, is one of the leading causes of improper payments" (Marsden and Berry, 2004).

Improper Payment Pilot Test Studies

At the request of an entitlement agency, LexisNexis has conducted three pilot projects to test for potential inadvertent and intentional errors (purposeful misrepresentations) and fraud among beneficiaries. Three separate programs both

[1] Centrelink was established in 1997 as a "one-stop shop" for integrated access to Australian government services. (GAO-02-69G)

under the auspices of this agency, were used to assess the susceptibility of improper payments. Several factors that may result in errors were measured, including address changes, mis-keyed input data, fraudulent addresses, or ineligible individuals and companies.

Methodology

Each program provided 1,000 individuals randomly selected from the most recent two months of initial claims. The risk of fraud or error was determined using LexisNexis InstantID, an online identity authentication service used by banks to validate and verify the claimed identity of new customers.[2] While it is a generic model designed specifically for identity authentication and not improper payments, it was employed to provide insight into the problem. Each potential recipient received a score on a scale of 0 (highest risk) to 50 (lowest risk, which was based on 13 levels of verification. The scores, including an interpretation, were provided to the two organizations. The two programs were then responsible for reviewing them and following up on the individuals who were placed in the high risk categories. After further investigation, the organizations reported back on the accuracy of the risk scores.

Findings

Program A

The observations from Highest Risk Cases provide some insight into the problem, including the need for greater access to data, and the benefits of information sharing. When the combination of Last Name/Address/SSN/Phone was searched, nine (9) individuals had identifiers that were not found together in the databases checked. The analysis of the identifiers determined that the individual data points were valid, but nothing tied the information together, thus scoring the risk of fraud or error at the highest level. Follow up analysis by the program found that all data was verified as accurate.

The assessment found that the SSNs of 17 individuals were not found in the public record databases. The explanations for these anomalies were that they were new SSNs, the SSNs were mis-keyed by several digits, or they were fraudulent. Follow up analysis by the program confirmed that 13 of 17 were new SSNs and four were mis-keyed.

Table 1: Recipient Verification Index for Program A Sample (n=1000)

Score	# Individuals	Percentage	Risk Level
0	14	1.4%	Highest
10	22	2.2%	High
20	229	22.9%	Moderate
30 or 40	735	73.5%	Low

Program B

In this pilot, a number of anomalies were identified when the Name/Address/SSN combination was assessed. The potential risks included: (1) 49 Individuals not found; (2) 29 individuals SSN found but with different Name & Address; (3) 17 matched Last Name & Address only, and (4) 314 found with matching Name & SSN but with different Address. When Name/Address/Phone (N/A/P) was used, 195 individuals N/A/P were not found and 114 individuals' phone were found but with a different Name & Address.

In this pilot study, the risk categories were refined to better reflect the degree of risk. This entailed expanding the risk categories from five to six levels.

Table 2: Recipient Verification Index for Program B Sample (n=1000)

Score	# Individuals	Percentage	Risk Level
0	21	2.1%	Highest
10	98	9.8%	Higher
20	180	18.0%	High
30	152	15.2%	Moderate
40	153	15.3%	Low
50	396	39.6%	Lowest

Program C

The higher risks were identified based on discrepancies in the information provided. Phone verifications were valid for 897 cases and problematic for 103 individuals. Of the phones not verifiable, 32 were categorized as missing, invalid, mobile or pager, and 46 phones were associated

[2] InstantID® was designed by LexisNexis® RiskWise® and the ABA to help financial institutions comply with the new account opening procedures required by Section 326 of the USA PATRIOT Act. InstantID verifies information across multiple databases using a powerful search process. InstantID validates that such information as name, address, date of birth and social security number are authentic and identifies potentially high-risk data elements, such as prison addresses, campground addresses, disconnected phone numbers, Social Security numbers of deceased persons, etc. Additional information on InstantID® is located at http://www.aba.com/cab/cab_instantid.htm.

Table 3: Recipient Verification Index for Program C Sample (n=1000)

Score	# Individuals	Percentage	Risk Level
0	17	1.7%	Highest
10	61	6.1%	Higher
20	149	14.9%	High
30	164	16.4%	Moderate
40	193	19.3%	Low
50	416	41.6%	Lowest

with different name and address. Out of the 1000 cases, 950 SSNs were verified. Of the 50 that were not, five were classified as missing or invalid and 50 were associated with different name and address. Address verification found 32 anomalies with five address either missing or not valid and 26 associated with a different name.

Pilot study C added a new dimension to determine if applications taken over the phone were any different than ones submitted via the Internet. Table 4 indicates a slightly higher risk of telephone applications as compared to those submitted via the Internet.

Table 4: Program C Application Method and Risk

Risk Level	Internet	Telephone	Combined
High	19%	26%	23%
Medium	16%	17%	16%
Low	65%	58%	61%

Discussion

The results of the three studies must be viewed with considerable caution. As can be seen from the program follow up, the "High Risk" categories do not necessarily indicate that there is fraudulent behavior. Rather, they suggest that the individuals' information requires greater checking. As can be seen in the second pilot test, there are reasonable explanations for the anomalies.

It appears that, at a minimum, a sizeable number of recipient data is not current and may be mis-keyed. The percentage of the combined highest levels of risk in the three studies, 3.6%, 30% and 23%, indicates the potential for sizeable inadvertent and intentional errors, as well as fraudulent behavior in the three samples. While further research must be conducted in this area and the methodology refined, it appears that this approach provides a great deal of promise for ferreting out improper payments on a large scale where identity problems and eligibility weaknesses are a cause. It will also significantly reduce costly errors, both inadvertent and intentional, that provide opportunities for fraud and abuse.

The anecdotal cases and pilot studies indicate a need for further research in order to ascertain the impact of identity fraud/theft as a cause of improper payments. A custom model design that includes broader data sets, greater refinement of the analysis, and increased information sharing will clearly yield more robust results. This will allow for greater segmentation of the risk and a more effective application of scarce resources to mitigate improper payments.

♦♦♦

Part III

Applying Risk Assessment Methodology to Improper Payment Management

Risk Assessment

The use of risk assessment in government and national security has grown tremendously in the last few years and has been applied to the improper payment problem. In an October 2003 GAO report (GAO-04-99), one recommendation was to "develop detailed plans to determine the nature and extent of possible improper payments for all agency programs and/or activities spending federal funds." In order to develop these plans, a risk assessment is critical.

> An essential element of developing an action plan is the completion of a risk assessment, which can be used to prioritize time and resources and set error rate reduction targets. A risk assessment is a key step in gaining assurances that programs are operating as intended and are achieving their expected outcomes. It entails a comprehensive review and analysis of program operations to determine where risks exist, what those risks are, and the potential actual impact on those risks on program operations. (GAO, 2003, pp.11 and 12)

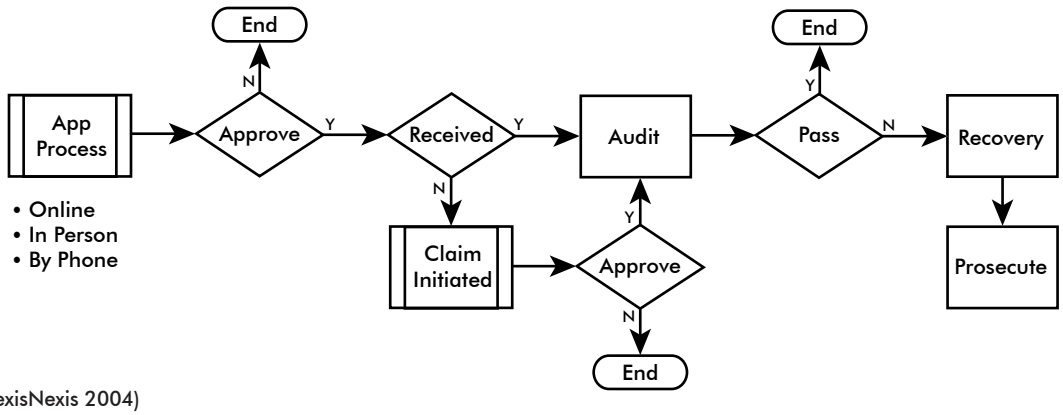
The report identifies the importance of risk assessment in the overall process of preventing and controlling improper payments. "… risk assessments set the stage for the identification, design, and implementation of control activities to address the causes of the problem" (Ibid, p.15).

The risk assessment process must be repetitious so that new problem areas will be identified and adapting criminals will be detected. "As further risk assessments are completed and potential improper payments are identified, additional controls can be developed and implemented to target these problem areas. (Ibid, p. 18).

Figure 1: *Entitlements Flow* illustrates the general components of an entitlement payment process. It can aid in a risk assessment by identifying the risk for improper payments at various stages of the process.

A strong eligibility assessment is essential during the application process, as it is a point of high risk. Two additional means of mitigating the risk of improper payments are periodic audits of the individual cases and an oversight process for the entire system. During the periodic audits, the status of an awardee can be checked and a determination can be made regarding the benefits currently received. This will ensure that fewer improper payments are made and may allow for the recovery of those already paid. By reviewing terminations, individuals who were wrongly terminated can be identified, and lessons learned can be drawn from the files of those who were terminated for cause. The audit process may include statistical sampling of data at various stages, e.g. enrollment and post award, to determine if there are risks that need to be addressed.

Figure 1: Entitlements Flow
General Overview of Payment Outlay



(Source: LexisNexis 2004)

Identity Authentication (individual and entity) as a Risk Assessment and Risk Mitigation Strategy

Objectives of Identity Authentication

The objective of identity authentication is to create a credible deterrent to identity theft and falsification (false identifiers and fraudulent documentation). At the most basic level, exposing the criminal intent of an individual before any damage has occurred is the optimum. The process can be likened to traditional intelligence gathering, but with different "analytic" tools and information sets. Information-based authentication strives to achieve the following goals:

- Prevent the use of false or assumed identities as a means to facilitate improper payments.
- Prevent the financial exploitation of the government

Information-Based Authentication Process

The term authentication originated in the information technology discipline, but has migrated to reflect the ability to verify people using various methods: knowledge, token, or biometrics. As the availability of public, commercial and government data has increased, the ability to authenticate identities using knowledge-based (information) systems has improved correspondingly. In response to this freer flow of personal information, various policy regulations have been enacted to address privacy issues, including access, accuracy, storage, notification, redress, and security.

Information or knowledge-based authentication is the foundation of identity authentication as it is scalable and cost-effective. Biometric and token-based authentication systems can be added to this first tier approach as the risk increases. The inclusion of these authentication technologies in a multimodal approach will enhance the effectiveness of agencies that administer high-risk entitlement programs.

A typical information-based authentication process includes multiple steps: validation, verification, high risk detection, and statistical modeling. These steps are listed in increasing sophistication and, as a result, have increased costs associated with their implementation. Generally speaking, as the perceived risks increase, the methods used to prevent and control them must be more sophisticated. Below are summaries of the steps:

Validation: A process that determines if data (e.g. address, phone, social security number) are real. At this level, there are two concerns.

- Do the specific personal identifiers presented, e.g. address, phone, and SSN, exist?
- Are the elements in the appropriate format as identified by the issuer of the data (e.g. driver's license and social security number)?

Verification: A process that determines if data belong together and determines if information supplied is the best available information.

- As an example, can the name, address, telephone, and SSN be confirmed together in multiple data bases? Through parallel searching/matching?
- Are there keying errors?
- Is data accurate based on best available data?

High Risk Detection: A process that determines if data components (i.e., address, telephone, SSN) are potentially higher risk.

- Address = prison, campground, non USPS or Commercial Mail Receiver
- Telephone = cell phone, pager, disconnected, out of plausible range
- SSN = deceased, multiple holders

Statistical Models: The application of analytics to known risky and normal individuals to detect patterns in authentication data that is indicative of risk.

- A composite of many elements that returns a single probability that a person is not who they say they are. In other words, the information presented about that person indicates a higher risk.
- Can include multimodal information sources (e.g. biometrics and data)
- Requires known behavior and authentication data on reasonably large samples of individuals

The pilot test data, anecdotal cases, and the risk assessment experiences of organizations such as Centrelink indicate that identity authentication is a critical aspect and a best practice of risk assessment and risk mitigation strategies. The challenge is to adapt proven existing methods and models or to develop new ones to mitigate risk of improper payment. Some of these methods and models will be applicable to all agencies and others will need to focused on the particular requirements of individual agencies.

The commercial sector has successfully used these best practices to prevent and control financial crimes. While the actual application of these techniques seems obvious today, in reality, authentication systems have been evolutionary, meeting the rising threat from ever-more sophisticated criminals.

Eligibility as a Risk Assessment and Risk Mitigation Strategy

While each agency's eligibility requirements may be different, the eligibility assessment process should be the same. First, each agency must articulate the eligibility criteria for each program. The second step will be to determine how the criteria can be mapped to commercial and government information to assist in decision making, especially during the enrollment phase. The next step is to determine if the information can be shared, based on law, a memorandum of understanding, and/or a privacy policy that is in place. If the responses to the second and third steps are positive, the criteria need to be incorporated in the model and access to the information must be procured from commercial entities or the appropriate government agencies.

The use of financial data, specifically income verification, would capture inadvertent and intentional errors, thus enhancing the decision making methods of many agencies. For example, this would catch individuals who misrepresented their income when they applied to an entitlement program. One area in which this concept is being tested is the student loan program within the Department of Education. "The Administration is analyzing options for improving income verification of student financial assistance programs while providing security and protecting taxpayer privacy. ED and Treasury recently conducted statistical test matches to estimate the savings that might result from ED's use of tax data to prevent overpayments to student aid applicants." (Office of Management and Budget, 2002).

Table 5
A Sampling of Eligibility Criteria and Information Sources

Criteria	Commerical	Government
Age	X	
Address	X	
SSN	X	X
Income Level	X	
Documentation of Medical Condition		
Documentation of Education	X	
Death Notice	X	
Attendance at College	X	
Proof of U.S. Citizenship		X
Veteran Status		X

Post Award, Audit, and Oversight

While much of the focus of this white paper has been on the enrollment phase, many of the same methods and models will be applicable to the post award and oversight phases. Once the identity authentication and eligibility assessment methods are refined, they will be applicable to other entitlement stages, as depicted in Figure 1: Entitlement Flow.

♦♦♦

Part IV
Challenges and Recommendations

Challenges

Leadership

The nature and complexity of entitlement agencies, covering both federal and state levels, makes it difficult to coordinate a comprehensive effort. This results in several good but fragmented approaches. Strong leadership at the highest levels is required to apply the best practices across the entitlement enterprise.

Limited research

After an exhaustive search, there appears to be little publicly available research on improper payments and its causes. A few pilot studies have been conducted to determine the size and scope, identity potential causes, and determine solutions for improper payments. These studies are not widely shared outside of the agency conducting the study.

There is no nationally funded research agenda in this area. Academic and think tank researchers have not focused their efforts on improper payments. Funding and access to data are two key limiting factors. Most of investigations into the problem have been conducted by the Government Accountability Office (GAO) and internal Inspector General's Offices of various agencies. These studies have highlighted the problem and evaluated the efforts by government agencies to reduce improper payments.

Limited information sharing among agencies

Information based identity authentication systems rely on information sharing policies that provide necessary information, while protecting an individual's privacy. Although there may be specific reasons for each governmental agency to deal with its own internal improper payment problems, a stove pipe approach is not in the best interest of the government or the American people. One example of information sharing between and among agencies is the cross verification of SSNs (O'Carroll 2004).

Information Based Identity Authentication systems can thwart attempts to defraud multiple organizations if the information can be shared. Individuals and criminal groups benefit from the lack of information sharing among organizations. They generally seek out vulnerable systems and use the same modus operandi to exploit them. Previous white papers have documented this phenomenon (Willox and Regan 2002) and (Gordon and Willox 2003).

Scalability

Improper payment solutions must be scalable to very large systems. They must be fast (near or real time), effective, and cost efficient. The analyses produced must be precise and hone in on the highest risk anomalies. Most agencies are faced with limited personnel resources and therefore, do not have the staff or expertise to track large numbers of potential risks.

Applying proven risk assessment methods and developing new policies, standards, and methods

In the Improper Payment Information Act of 2002, Congress requires the use of risk assessment methods in determining the size and scope of the problem and root causes of improper payments. However, no standardized method of risk assessment is proposed. The suggested methods range from relatively simple to very sophisticated. In addition, there is little discussion of implementing risk assessment strategies for near or real time decision making.

Some agencies have worked with commercial entities to assess whether the solutions generated for the private sector's problems can be applied to improper payments. These pilot studies have been limited in scope, but have provided insight into the problems faced by entitlement agencies.

Limited identity authentication systems

Intake/gatekeeper staff do not have access to sophisticated identity authentication systems to assist in the decision making in the enrollment phase. Such access would provide another screening tool to aid in the due diligence process. In order for such tools to be effective, the existing identity authentication systems must be adapted to the requirements and needs of various agencies. The effectiveness of the tools must be proven, so that they will be widely accepted.

Privacy concerns

As with other identity authentication programs, it is critical that policies be developed to balance the effective use of information with the privacy of individual citizens. As evidenced by some government programs, it is essential to consider policy and privacy in planning program development, information architecture development, and information technology programs.

Recommendations

Recommendation 1: Gain commitment from the Administration to lead a comprehensive federal and state effort to reduce improper payments significantly.

Congress has provided leadership through the Improper Payment Information Act of 2002. However, a coordinated and comprehensive federal and state plan must be put in place to manage the next steps of such a large and complex problem. It is evident that the goals of the Improper Payment Information Act of 2002 cannot be met if federal and state agencies work independently of one another.

A comprehensive strategy will allow for the application of best practices across all levels of government. While there are multiple entitlement agencies with very specific differences, the similarities of the entitlement and payment processes should allow for the sharing of the best-of-breed methods, policies, and technological solutions.

Recommendation 2: Apply proven risk assessment methods and best practices to improper payments.

While the application of risk assessment methods has been a long time practice in the private sector, it is a relatively new approach for government organizations. The application of risk assessment to a wide range of government and national security issues has dramatically increased in the past three years. The core concepts and applications developed by the private sector provide a good starting point for the problems faced by government. Pilot studies afford industry and government the opportunity to adapt proven methods, developed for other purposes, to problems such as improper payments. These public-private sector partnerships should be encouraged, as they will facilitate the rapid development of new strategies and solutions for improper payments.

As a result of the mandates of the Improper Payment Information Act, agencies will be applying risk assessment methods to their specific improper payment problem areas. These experiences should be studied to ascertain the best methods and practices for improper payment risk assessment. The successful efforts should be shared across federal and state agencies.

Often, administrators are asked to develop risk assessment procedures in their organizations without the proper background information and subject matter expertise. It is recommended that courses, conferences, and executive seminars in risk assessment be offered to executives and mangers who are responsible for risk assessment in their agencies, so that they can develop new skill sets and competencies.[3]

Recommendation 3: Develop identity authentication systems that include eligibility assessment capabilities.

Identity authentication systems that include eligibility assessment and apply directly to improper payments need to be developed. Proven identity authentication systems developed for other purposes, such as the financial service industry and national security, can be applied to the improper payment problem. Pilot studies, such as the ones presented in this white paper, should be encouraged to determine the efficacy of using identity authentication systems for various stages of the improper payment process, including enrollment, post award, and oversight.

Initially, the focus should be on studying the use of information based identity authentication (knowledge based authentication). In areas where a greater risk of improper payments occur, it may be necessary to apply a multimodal approach that combines information based identity authentication and biometrics.

Recommendation 4: Establish a national improper payment research agenda.

Currently, there is little funding for academic studies in improper payment areas, such as risk assessment best practices, causes, fraud, identity theft, information sharing, and policy development focused on privacy. The research

[3] For example, Utica College, in conjunction with key personnel at the Department of Homeland Security, has established a four course graduate risk assessment certificate that is offered to DHS staff only.

that has been completed to date has been limited to GAO studies, which provide a good roadmap of the improper payment problem, but do not identify causes or solutions.

In addition to academic research, collaboration between industry and specific agencies should be continued and encouraged. Such collaboration can provide metrics for potential solutions to aspects of the improper payment problem.

Recommendation 5: Establish more sophisticated information sharing systems that incorporate the use of technologies such as distributed networks, while enhancing policies on privacy and information ownership.

Many of the recommendations in this study will not work without the development of clear policies and standards. There are many examples of government risk assessment efforts that have not succeeded, because of limited attention paid to use of information and privacy policies. Committees to study the use of information, information sharing, and privacy, for the purpose of developing standards and best practices, should be created.

The sharing of information between and among agencies should be studied and encouraged where it is determined that it can help prevent improper payments and where acceptable use policies can be developed. Such a program already exists between two agencies; however, the entire group of entitlement agencies could benefit from increased information sharing.

The sharing of information between agencies and industry should be studied to determine how sharing of information can assist in mitigating improper payments. For this to work, clear polices and standards for the responsible use of information must be articulated. Special attention must be paid to balancing the mandate to reduce improper payments and the privacy of the individual applying for and receiving an award from an entitlement program. One of the key factors is proportionality. This approach requires the use of only the necessary data to make an effective decision.

Any risk assessment system must incorporate information effectiveness capabilities with information sharing technology. Information effectiveness focuses on the quality of data sets employed for decision making. Understanding the limits of specific data sets, especially those with high error rates, can assist the organization in determining the value of the output. Coupled with this approach is the need to develop policy based information sharing technologies. Once these policies are established, the IT architecture can be designed. This will insure that policies, especially those concerning privacy, will be followed, and that an audit trail will be generated for oversight purposes.

The recommendations above must be fully tested and evaluated. Those programs that demonstrate promise should be designated exemplary programs. Funds should be made available to encourage their widespread use on both the federal and state level.

♦♦♦

Conclusion

Improper payment losses continue to grow at an astounding rate. However, it is encouraging to note that renewed efforts are being made to understand the causes and develop solutions to mitigate improper payment. The application of proven methods of risk assessment, identity authentication, and eligibility assessment offer real promise to reducing the significant losses suffered by entitlement agencies. These approaches require a strong partnership between government and private industry, which must work collaboratively to find new ways to use commercial data, solve critical policy and standards issues related to the use of data and privacy, and apply state-of-the-art technological solutions to a complex problem of great magnitude.

Strong leadership is essential to the development of a comprehensive federal and state improper payment plan. A robust research agenda must be facilitated, information sharing networks developed, and the application of proven methods and best practices encouraged or required. Those solutions that provide the widest impact, thus allowing for the management of scarce resources, should be given highest priority. It is only through a comprehensive and well orchestrated effort that improper payments can truly be reduced.

♦♦♦

References

Gerow, Charles. (2004). Testimony on Improper Payments. Retrieved September 27, 2004 from http://reform.house.gov/UploadedFiles/Gerow%20Testimony%20-%20Improper%20Payments.pdf

Gordon, Gary and Wilox, Norman (2003) Identity Fraud: A Critical National and Global Threat. Retrieved September 23, 2004 from Economic Crime Institute at Utica College Web site: http://www.ecii.edu/identity_fraud.pdf

Marsden, Thomas and Berry, Reginald (2004). Preventing Improper Payments: Leveraging Data & Risk Modeling Solutions. An unpublished white paper.

O'Carroll, Jr. Patrick. Enhancing Social Security Number Privacy. Retrieved September 19, 2004 from http://www.ssa.gov/oig/communications/testimony_speeches/06152004testimony.htm

Office of Management and Budget (2002a). The Improper Payment Information Act Public Law No: 107-300. Retrieved September 21, 2004 from www.whitehouse.gov/omb/memoranda/mo3-13-attach.pdf

Office of Management and Budget (2002b). The President's Management Agenda. Retrieved September 21, 2004 from www.whitehouse.gov/omb/budget/fy2002/mgmt.pdf

Risk Assessment for Improper Payments (FWS 3-2272). Retrieved September 16, 2004 from http://forms.fws.gov/3-2272.doc

Springer, L. (2004) Statement Before the Subcommittee on Government Efficiency and Financial Management. Retrieved September 21, 2004 from www.whitehouse.gov/omb/legislative/testimony/springer/040415_springer.html

U.S. General Accounting Office. (2001). Strategies to Manage Improper Payments: Learning from Private and Public Sector Organizations. (GAO-02-69G)

U.S. General Accounting Office. (2003). Financial Management: Status of the Governmentwide Efforts to Address Improper Payment Problems. (GAO-04-99)

Appendix: Entitlement Programs

1. Department of Agriculture	1. Food Stamps 2. Commodity Loan Program 3. National School Lunch & Breakfast 4. Women, Infants, and Children
2. Department of Defense	5. Military Retirement 6. Military Health Benefits
3. Department of Education	7. Student Financial Assistance 8. Title I
4. Department of Health & Human Services	9. Head Start 10. Medicare 11. Medicaid 12. TANF 13. Foster care – Title IV-E 14. State Children's Insurance Program 15. Child Care & Development Fund
5. Department of Housing & Urban Development	16. Low Income Public Housing 17. Section 8 Tenant Based 18. Section 8 Project Based 19. Community Development Block Grants (Entitlement Grants, States/Small Cities)
6. Department of Labor	20. Unemployment Insurance 21. Federal Employee Compensation Act 22. Workforce Investment Act
7. Department of Treasury	23. Earned Income Tax Credit
8. Department of Transportation	24. Airport Improvement Program 25. Highway Planning & Construction 26. Federal Transit-Capital Investment Grants 27. Federal Transit – Formula Grants
9. Department of Veteran Affairs	28. Compensation 29. Dependency & Indemnity Compensation 30. Pension 31. Insurance Programs
10. Environmental Protection Agency	32. Clean Water State Revolving Fund 33. Drinking Water State Revolving Fund
11. National Science Foundation	34. Research & Education Grants & Cooperative Agreements
12. Office of Personnel Management	35. Retirement Program (Civil Service Retirement System and Federal Employees' Retirement System) 36. Federal Employees Health Benefits Program 37. Federal Employees' Group Life Insurance
13. Small Business Administration	38. 7(a) Business Loan Program 39. 504 Certified Development Companies 40. Disaster Assistance 41. Small Business Investment Companies
14. Social Security Administration	42. Old Age & Survivors' Insurance 43. Disability Insurance 44. Supplemental Security Income Program

(Source: OMB Circular No. A-11, 2002)