3-27-2008

Attributes of Identity Document Credibility: A Synthesis of Expert Knowledge

Kenneth Robert Henry
Florida International University, henryk@fiu.edu

DOI: 10.25148/etd.FI08081524

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

ATTRIBUTES OF IDENTITY DOCUMENT CREDIBILITY:

A SYNTHESIS OF EXPERT KNOWLEDGE

A dissertation submitted in partial fulfillment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY

in

BUSINESS ADMINISTRATION

by

Kenneth Robert St. Leger Henry

2008

To: Dean Joyce Elam
College of Business Administration

This dissertation, written by Kenneth Robert St. Leger Henry, and entitled Attributes of Identity Document Credibility: A Synthesis of Expert Knowledge, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Dasaratha Rama

Kaushik Dutta

Debra VanderMeer

John Zdanowicz

Richard Tardanico

Ronald M. Lee, Major Professor

Date of Defense: March 27, 2008

The dissertation of Kenneth Robert St. Leger Henry is approved.

Dean Joyce Elam
College of Business Administration

Dean George Walker
University Graduate School

Florida International University, 2008

DEDICATION

I dedicate this thesis to my wife Marcella, who never let me lose sight of the importance of completing this journey, and to my parents: my father Kenneth, who instilled a boundless curiosity about how things work, and why the world is the way it is; and my late mother Hilda, who always told me to aim for the stars. Without their patience, support, and most of all love, this work would not have been possible.

ACKNOWLEDGMENTS

I wish to thank my committee members for their support, patience, and unfailing good humor in making sure that this document was completed according to their high expectations for quality. I appreciate very much their suggestions and directions. In particular, my major professor, Dr. Ronald Lee, was willing to take the risk of letting me find my own research path, although it led to unfamiliar territory for him. From the very beginning, he showed confidence in my ability to complete the degree with excellence, pushing me firmly when I moved too slowly.

I found my coursework throughout the PhD program to be stimulating and thought provoking, providing me with tools and techniques to explore new research ideas, and so I thank my course professors.

On the personal side, my thanks to all the friends and family members who encouraged me, with special acknowledgment to those who gave so willingly of their time and expertise by

(1) acting as my audience for formal presentation rehearsals: Deborah Chen, Richard Foster, Mark Gapski, David Murray, and Julia Niarchos, and;

(2) assisting me with legal research and manuscript editing: Jacqui Foster, Noel & Monica Heron, and Cherol Ramsay,.

Finally, I am grateful to all my students, past and present, especially those who served as student Accounting Association Executive Board members during the time I struggled to complete this document, and still meet my commitments as their faculty advisor. You all played a significant part, first as student leaders, and now as professionals, in exercising patience, yet giving me constant encouragement as I worked my way through the PhD process.

ABSTRACT OF THE DISSERTATION

ATTRIBUTES OF IDENTITY DOCUMENT CREDIBILITY:

A SYNTHESIS OF EXPERT KNOWLEDGE

by

Kenneth Robert St. Leger Henry

Florida International University, 2008

Miami, Florida

Professor Ronald M. Lee, Major Professor

In broad terms — including a thief's use of existing credit card, bank, or other accounts — the number of identity fraud victims in the United States ranges 9-10 million per year, or roughly 4% of the US adult population. The average annual theft per stolen identity was estimated at $6,383 in 2006, up approximately 22% from $5,248 in 2003; an increase in estimated total theft from $53.2 billion in 2003 to $56.6 billion in 2006. About three million Americans each year fall victim to the worst kind of identity fraud: new account fraud. Names, Social Security numbers, dates of birth, and other data are acquired fraudulently from the issuing organization, or from the victim then these data are used to create fraudulent identity documents. In turn, these are presented to other organizations as evidence of identity, used to open new lines of credit, secure loans, “flip” property, or otherwise turn a profit in a victim's name. This is much more time consuming — and typically more costly — to repair than fraudulent use of existing accounts.

This research borrows from well-established theoretical backgrounds, in an effort to answer the question – what is it that makes identity documents credible? Most importantly, identification of the components of credibility draws upon personal construct psychology, the underpinning for the repertory grid technique, a form of structured interviewing that arrives at

a description of the interviewee's constructs on a given topic, such as credibility of identity documents. This represents substantial contribution to theory, being the first research to use the repertory grid technique to elicit from experts, their mental constructs used to evaluate credibility of different types of identity documents reviewed in the course of opening new accounts. The research identified twenty-one characteristics, different ones of which are present on different types of identity documents. Expert evaluations of these documents in different scenarios suggest that visual characteristics are most important for a physical document, while authenticated personal data are most important for a digital document.

TABLE OF CONTENTS

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

FIGURE PAGE

I. FOREWORD

Author's background. This career spans 35 years in the accountancy profession, including education in both accountancy and computer science, and twenty years of auditing experience. Entering the PhD program was expected to complete the transition from commerce & practice to education & research. So often in the accountancy profession, practitioners find themselves frustrated, as they try persuading bosses and colleagues to adopt intuitive solutions to pragmatic business problems. Practitioners and consultants lack the qualitative and quantitative evidence of theoretical research, denied by time and resource constraints set by economic and profit objectives. Conversely, educators and researchers develop materials strong on theory, but untested in the arenas of commercial and professional sustainability.

Educators are ultimately responsible for preparing students, and through them, the business community, to face the economic, technical, political, and scientific challenges that lie before us. Who could be better than those with both the pragmatic perspective of significant work experience in business and industry, and the intellectual perspective of disciplined theoretical research and publication? In preparing for this transition from practice to scholarship, and looking forward to the new role as researcher and educator, it is important to keep the practical implications at the forefront.

After exploring the potential of a wide variety of different ideas and interests, this optimal balance between research and practice has been the beacon for settling into the eventual course taken by this dissertation research.

II. INTRODUCTION

The Global Implications of Identity Fraud

The largest case of identity fraud in U.S. history (FBI, 2004), at least through 2004, began with a crooked "insider" who had access to a nearly unending supply of personal consumer information. It ended up being the largest case of identity theft ever investigated and prosecuted in the United States --with criminal ringleaders in Nigeria, 30,000 victims across the U.S. and Canada, and millions of dollars in losses.

Clearly, there is a need for better ways of preventing and detecting identity fraud -- and that is the reason for this research! The goal is to give organizations a tool that they can use to recognize the crime when it is attempted, rather than waiting to "clean up the mess" after it has occurred -- prevention rather than detection. And of course, the individual victims of identity fraud would prefer never to have become victims in the first place.

Organization of This Document

The main body of this document is organized into nine sections.

1. Introduction. This first section gives the document overview and a brief description of the author's research journey, a description of some of the contributing disciplines that have evolved from personal experience, and a description of the type of contribution to be made.

2. Motivation and Background. This sets the stage for the proposed research, giving some details of the crime of identity fraud, the research objectives and benefits, the expected contribution, and the deliverables produced by the research.

3. Identity Fraud. Here is a description of the different types of identity fraud, its extent, and some of its characteristics, along with descriptions of how it is typically accomplished. Finally, it

contains some discussion of the existing work being done in the areas of law enforcement, legislation, and ongoing research.

4. Credibility. This section reviews the relevant literature and summarizes relevant research in related concepts and different contexts, discussion of how credibility is evaluated, and finally how it is defined for this research proposal.

5. Contribution. This section discusses the research model describes the specific deliverables produced by the research.

6. Theoretical Perspective. Describes the theoretical background for the research methods planned, with discussion of the repertory grid.

7. Methodology. This section contains the results of the repertory grid interviews, with discussion of how results are evaluated.

8. Summary of Results. This describes the results and provides a discussion of how these results lead to the contribution generated by the research.

9. Future Research. Some directions for future research are considered here.

Contributing Disciplines - The Research Journey

Audit Patterns. This research quest began with the idea of "audit patterns" as a technique for researching the problem of auditing controls in an inter-organizational environment. What if we could have recognized the 1994 Eiffel Tower incident below, as an audit pattern in a knowledge repository of potential terrorist threats? At a global level, many unrelated organizations have high levels of interest, large knowledge pools, and yet do not communicate effectively. If there were some way of pooling their knowledge, to create an “audit pattern”, the disaster might have been avoided. The threat pattern is: fly an airplane into a national monument. Some apparently unrelated knowledge items are:

- 10 Jul 1981 - The film “Escape from New York” debuts in American theaters. The movie begins with terrorists taking control of Air Force One and suicidally crashing it into a New York City skyscraper.
- 24 Dec 1994 - Four armed terrorists from the Groupe Islamique Armé (GIA) hijack Air France flight 8969, with the intent of crashing it into the Eiffel Tower. The plane is finally stormed 48 hours later by French soldiers at Marseille International Airport.
- 1999-2001 - NORAD plans and executes drills on how to defend the country against attacks by terrorists using hijacked airliners as missiles. A proposed drill with an airliner crashing into the Pentagon is scrapped as "unrealistic."
- 11 Sep 2001 – terrorists fly hijacked airliners into New York’s World Trade Center

What if the local police in Florida could have used such a knowledge repository of audit patterns to recognize the 9-11 terrorists doing their flight training? It is easy to talk about this knowledge repository of audit patterns, but not so easy to say what this knowledge repository would look like. Where would the inputs come from, and how would it be updated accurately and securely?

Money Laundering. And so the research goal changed from terrorist threats to money laundering. However, it became clear that it would be difficult to describe money-laundering patterns. It is difficult to size the money-laundering problem, and in fact, most instances of money laundering go mostly undiscovered, which would have made it very difficult to get specifics on the observed patterns. However, the thinking about money-laundering lead to recognition of identity theft as a more tractable problem, and also one that seemed interesting for the author’s professional experience.

Identity Fraud. Currently, the most commonly cited definition is provided in the 1998 Federal Identity Theft and Assumption Deterrence Act. It considers an individual to commit an act of identity theft when he or she "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law." (Identity Theft and Assumption Deterrence Act 1998). However, for this research the working definitions of identity and the potential for identity fraud are as follows. Identity is a set of facts about the relationship between an individual and an organization, recorded on an identity document or identity token -- so that the organization can correctly connect the individual with his or her authorized affordances. The research interest is to explore the potential for identity fraud, which is therefore defined as a situation where the identity document does not correctly represent its holder. To clarify the point, consider the question of whether changing your own facts on your own identity document counts as fraud. The answer is that whether or not it constitutes fraud, the changing of your own facts is an indicator of fraud potential, which is the variable of interest.

The identity fraud process is described very well in the literature, for example (Willox Jr., Gordon, Regan, Rebovich, and Gordon, 2004). Their overview is reproduced below as Figure 1. However, the process is summarized for this research as the A-B-Cs of identity fraud.

A-Acquisition of the identity data – a minimal data set for a stolen identity document is the consumer's name, date of birth, and social security number.

B-Breeding new identity documents – the thief uses the acquired identity data set to "breed, i.e., fraudulently apply for – other documents such as a driver's license with data that does not correctly represent the fraudulent applicant. Breeding continues, to obtain "replacement" birth certificate and social security card, which in turn may provide additional data for the stolen

identity document, such as parents names, place of birth, and so on. Other fraudulent identity documents can be purchased on the "black market." Each document created by the breeding process is a real document in the sense that it has been issued by the providing organization, and not subsequently altered or forged. However, the situation has a high potential for identity fraud, as none of the documents correctly represent the fraudulent applicant. Each document produced by the breeding step is a real document in the sense that it is not altered or forged. However, it does not represent the holder — the situation described as the potential for identity fraud.

C-Conversion for financial gain – as the fraudulent but real identity documents accumulate from the breeding process, it becomes more difficult to discover the criminal identity. The thief improves the "credibility" of the fraudulent documents because all their data corresponds.

Regardless of the environment, one important phase in the identity verification process when only a knowledge-based solution can be used is at the beginning of the identity verification process. The individual is new to the verifier, and the verifier has had no previous contact with the individual. This stage of the identity verification process is most susceptible to abuse. Because biometric and token solutions, i.e., identity documents are not yet available at this phase of the identification process, there can only be a knowledge-based solution (Willox Jr. and Regan Esq., 2001) This is the approach to be taken in this research, to measure the credibility of the types of identity documents presented at the beginning of the verification process.

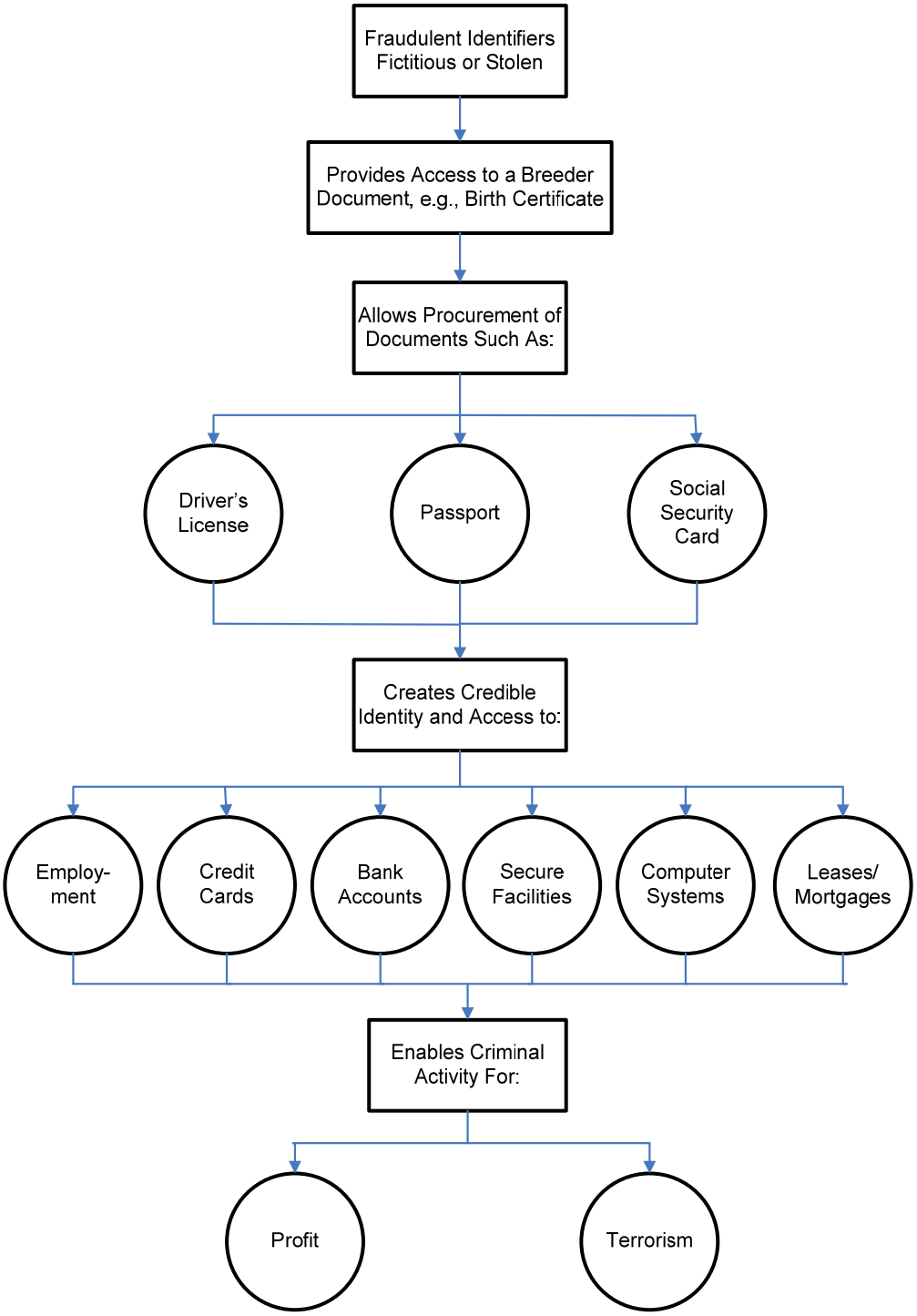

Figure 1. Identity Fraud Process

Inter-Organizational Risks. The inter-organizational problem of identity fraud also merits discussion. As each individual receives a token from one organization, and presents it to another, an inter-organizational network is created The traditional investigator (auditor, security analyst, risk manager, etc.) who has a long history of evaluating risk, as well as designing, implementing, and evaluating appropriate internal controls, typically would address the risks and security issues at an organization level. However, even the best efforts of these individual investigators may not be sufficient to prevent certain types of fraudulent identity documents from "falling through the cracks" between the individual member jurisdictions in an inter-organizational "space".

Artificial Intelligence Approach - Logic of Identity Fraud. What happens physically for the deception involved with identity fraud is that one organization creates a token, and updates an institutional registry. The individual takes this token, and presents it to another organization. The new organization relies on the validation of the previous one. What happens logically for the deception is that the individual, who never received a token from the first organization, presents a token anyway, for which there is no corresponding update in the registry, as the second organization relies on the assumed validation by the first organization. Although this approach to the identity fraud problem seemed interesting, it became clear that validation would be difficult and time-consuming to accomplish, and so this research has been postponed for future efforts.

Engaged Scholarship. This is defined (Van de Ven, 2007) as a participative form of research to obtain the different perspectives of key stakeholders. Van de Ven writes, "By involving others and leveraging their different kinds of knowledge, engaged scholarship can produce knowledge that is more penetrating and insightful than when scholars or practitioners work on the problem alone." The approach taken in this research is to leverage the professional experience of financial service experts involved with evaluating identity documents presented

when new accounts are opened, to develop a list of the characteristics that make identity documents seem credible to them. The practitioners' experience is then used again to validate this list of characteristics, to rate the importance of each characteristic in each of four different scenarios.

Setting the Research Boundaries. This research is focused on how bank Customer Service Representatives make their decisions about accepting (or not) an identity document presented by a potential customer coming into the bank to make a new account application. This represents a departure from the more usual focus seen in the research literature on identity theft and identity fraud; on the victims and reparation, the perpetrators and investigation, the security and prevention, tamper-resistance and detection, and the regulation and law enforcement. However, when all is said in these areas, the business problem that confronts any bank is one of balancing profitability with risk. As for any other business, correctly accepting potential new customers is critical to a bank's profitability and survival. Too many false positives -- accepting a fraudulent identity -- will result in overwhelming fraud losses. Too many false negatives -- rejecting a fraudulent identity -- will result in lost revenues as potentially profitable new customers are turned away.

This focus on the persons making decisions on the documents presented comes from more than 30 years of experience in evaluating documentary evidence, as a financial auditor and accountant. Often -- in trying to explain to an inexperienced audit colleague, or to an information system professional, how judgment and experience play a major role in evaluating the credibility of any kind of document -- the question would arise, of why using an IS-based or AI-based evaluation method should be difficult? A favorite example is a real experience in the early 1980s, as an audit manager with about 10 years experience at the time, walking into a new medium-sized client. Within an hour of walking around, looking at the operations, and talking to some of the

key executives, I felt a tingling in my spine, and the hair on the back of my neck stood up, and in my gut, I felt that there was going to be an audit problem with this new client. Sadly, it turned out that the gut reaction was well founded. The audit discovered an ongoing fraud, which turned out to be an embezzlement scheme that amounted to about $150,000 over two years. Even now, more than twenty years later, I cannot explain what I heard, or saw, or perceived in some way, that made me have the gut reaction I described, "We have a problem!" It is this gut reaction that I wanted to understand, what it is that makes experts on dealing with identity documents react positively or negatively when they see these documents in some specified scenarios.

The research journey ends with the development of answers to the question that lies at the heart of this dissertation. What is it that makes identity documents seem credible to the experts who evaluate them? In additional to the personal experience, much of the inspiration for this research comes from a few sources.

(1) Imaginative Theorizing (Locke, Golden-Biddle, Edmonton, and Feldman, 2004) -- to help create a new perspective for evaluating credibility in the context of identity documents and identity fraud.

> "*Inspirational resources ... [are used for] generating ideas ..., interpretive micro-processes [are applied to]... engage the data ... to select and shape the ideas ..., and a researcher stance ... actively seeking to create and explore multiple possibilities for understanding ...*"

(2) Engaged Scholarship (Van de Ven, 2007) -- the source for tying together the scattered ideas about the desire to blend industry experience with research methods.

> "*By involving others and leveraging their different kinds of knowledge, engaged scholarship can produce knowledge that is more penetrating and insightful than when scholars or practitioners work on the problem alone*."

(3) Boundary Critique and Systems Thinking (Cabrera, 2006) -- contributed an understanding of the need to create a concept map with boundaries, to guide the research direction and effort.

"*Systems thinking is a conceptual framework, derived from patterns in systems science concepts, theories, and methods, in which a concept about a phenomenon evolves by recursively applying rules to each construct ... until an internally consistent conclusion is reached. The rules are:*

-Distinction making: differentiating between a concept's identity (what it is) and the other (what it is not) [boundary critique],
-Relating: inter-linking one concept to another
-Systems [Organizing]: lumping or splitting concepts into larger wholes or smaller parts; and
-Perspective taking: reorienting a system of concepts by determining the focal point from which to observe other objects [point-of-view]."

(4) Design Science (Hevner, March, Park, and Ram, 2004) describes the possibility of a research contribution being a methodology or process, validated by even a single instantiation.

"*The result of design-science research in IS is, by definition, a purposeful IT artifact created to address an important organizational problem. It must be described effectively, enabling its implementation and application in an appropriate domain. ... We include not only instantiations in our definition of the IT artifact but also the constructs, models, and methods applied in the development and use of information systems*."

(5) Personal Construct Theory (Kelly, G., 1955) provided an answer to the search for a theory-based methodology to understand the world of an experts in their field.

"*One of the central assumptions of the [Personal Construct Theory] is that reality, and what we make of it, is built up of contrasts [constructs] rather than absolutes. A person's construct system is composed of a finite number of dichotomous constructs "*

And of course it was important to explore the literature related to identity theft and identity fraud, as well as the stream related to describing credibility in different settings.

As with any well-planned exploration, research or otherwise, it is important to describe where the journey begins, traverses, and ends. However, experienced travelers likely recognize that it may be just as important to describe, or at least list the paths NOT taken along the way. These will provide boundaries; a context for the description of the discoveries made during the journey and pointers to future explorers for new safaris and discoveries.

Here then are the paths not taken, the boundaries and limitations of the research scope.

- The broad domain for this research is limited to the financial services industry (banks and credit unions), although it is generalizable.
- The specific activity where risk is highest is when opening a new account – this is the specific domain for this research.
- Personnel selected as experts had a minimum of 10 years of experience.
- Some additional boundaries were set in limiting the number of elements in the repertory grid (twelve identity documents).
- This research focuses only on financial identity fraud. Chapter 3 discusses briefly, other types such as medical, Homeland Security, and Corporate ID Theft.
- Only the construct elicitation phase of the repertory grid method is used. Requesting more time from busy managers would have resulted in a much lower level of participation. The full grid analysis is deferred for future research.
- During construct elicitation with twelve elements, only 25 of 220 (12*11*10 / 6) possible triads were used, in order to limit the research interviews to approximately one hour in length. Again, longer interviews would have resulted in a much lower level of participation.
- Although six significant trends were identified (for 36 possible scenarios), they were grouped in two sets of three, to limit the research to four clearly defined and differentiated scenarios.

III. MOTIVATION AND BACKGROUND

What's the Problem? Crime of Identity Fraud

The problem to be examined involves the crime of identity fraud. In broad terms — including a thief's use of existing credit card, bank, or other accounts — the number of victims in

the United States ranges from nine to ten million per year, or roughly 4% of the United States adult population. No exact measure exists of the cost of identity fraud, but based on survey responses from victims, the average annual theft per stolen identity was estimated at $6,383 in 2006, up approximately 22% from $5,248 in 2003. This corresponds to an increase in estimated total theft from $53.2 billion in 2003 to $56.6 billion in 2006 (Javelin, 2006). About three million Americans each year fall victim to the worst kind of identity fraud: new account fraud. In these cases, names, Social Security numbers, dates of birth, and other data are acquired fraudulently in a variety of ways from the issuing organization, or from the victim. These data are then used to create fraudulent identity documents that are presented to other organizations as evidence of identity, used to open new lines of credit, secure loans, "flip" property, or otherwise turn a profit in a victim's name. This is much more time consuming — and typically more costly — to repair than fraudulent use of existing accounts.

The United States Department of Justice web site gives a horrifying example of one case of identity fraud.

> " *... the criminal, a convicted felon, not only incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but called his victim to taunt him -- saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time -- before filing for bankruptcy, also in the victim's name. While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, the criminal served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused. This case, and others like it, prompted Congress in 1998 to create a new federal offense of identity theft.*" (USDOJ, 2007)

So What? Significance of this Research

This research is significant for three reasons. First, describing the attributes of credible identity documents would allow better understanding of the indicators that should be the focus in developing solutions for the identity fraud problem. This is the primary focus of this dissertation.

Second, validating the credibility index as a metric for potential identity fraud would provide organizations with a tool to estimate identity fraud risk associated with any identity documents reviewed. Such a tool would also be significant to those responsible for investigation, regulation, and law enforcement related to identity management, and identity fraud. Third, there is an increasing number of entities that both create identity documents, and review documents created by other entities. This comprises an inter-organizational network whose ongoing growth makes it more complex, increasing the value and corresponding risk of fraudulent access to the individual network member information and assets, and increasing the need for identity document risk management.

Who Cares? Research Benefits

The idea is to provide the organization with criteria for evaluating the credibility of newly presented identity documents, according to what type of document is presented. Further research, beyond the scope of this document could even provide the organization with a method for setting policy on what types, and how many different types of documents to require for opening a new account.

What's the Point? Research Objectives

The research objective is to specify and measure these components of credibility, as related to the documents issued by one organization, and reviewed by another as evidence of a person's identity, in order to answer the questions of:

(1) What attributes do experts look for in identity documents when judging their credibility?

Describing attributes of credible identity documents allows better understanding of the indicators

of potential identity fraud that should be the focus in developing solutions for the identity fraud problem.

(2) Having specified the attributes, how do experts rate their relative importance?

Measurement of identity fraud potential can provide a tool for selecting most useful identity documents.

Also related to credibility is the notion of cognitive authority (Wilson, 1983). Both concepts include trustworthiness and competence as two of their main components. Only someone who is considered to "know what they are talking about" is recognized as a cognitive authority. Wilson claims that people do not attribute cognitive authority exclusively to individuals. Cognitive authority can also be recognized in books, instruments (such as a digital identity), and organizations. This notion of cognitive authority provides the basis for what makes a digital identity credible. If we can isolate these attributes of credibility, then (intuitively) we should be able to measure them.

The research goal is to measure credibility of identity documents, as a metric for potential identity fraud. This entails: (1) eliciting these attributes, or components, of credibility for each type of identity document, and then (2) rating the relative importance of each elicited attribute.

What's the Claim? Credibility Measurement Metric

The primary hypothesis posed, is that the measurement of credibility of different types of identity documents is a good metric for estimating the potential that the type of identity document being presented is in fact fraudulent; in other words, that measurement of identity document credibility is a good metric for potential identity fraud. Let's analyze that idea.

Under civil law, fraud is "the act of intentionally making a false representation of a material fact, with the intent to deceive, which is reasonably relied upon by another person to that person's detriment." According to the non-profit Identity Theft Resource Center, there are three main forms of identity theft: (1) Financial Identity Theft -- fraudulently using someone else's personal identifying information to obtain goods and services), (2) Criminal Identity Theft -- impersonating someone else when apprehended for a crime, and (3) Identity Cloning -- using someone else's information to assume a new identity in daily life (Foley and Foley, 2003). This research will focus only on the first of the three types described; it will be referenced throughout this discussion as identity fraud. Note that there are at least two victims: the consumer whose identity data has been stolen, and the commercial organization that loses unpaid goods or services. Recall that identity is defined as a relationship: in this case, between a person who has authority to access certain affordances such as goods, services, and information; and an organization, that has custody of these affordances, and is therefore obliged to limit access only to the authorized person.

For this research, the working definition for credibility actually has ancient origins. Aristotle, writing in the 5th century BC, discussed the notion of credibility in his examination of *ethos*, as he relates it to his observations of speakers' abilities to persuade listeners to believe them (Aristotle, 1991 translation). This view is retained today — Webster's New World Dictionary defines credibility as believability. Credible people are believable people; credible information is believable information (Fogg, Swani, Treinen, Marshall, Laraki, Osipovich, Varma, Fang, Paul, and Rangnekar, 2001). Credibility is a perceived quality, and there now appears to be some scholarly agreement that credibility has multiple dimensions including trustworthiness and expertise (Fogg and Tseng, 1999), that must be simultaneously evaluated.

Other researchers have focused on perceptions of "relative credibility", especially for comparisons between the Web and traditional news media (Roper, 1985). However, this does not really help to specify the *variables* that make one medium more credible than another (Nass and Mason, 1990), or the *processes* used in evaluating the different media types, or the *attributes* of a medium that aid in credibility assessment (Burbules, 2001). For this research, the definition for identity document credibility is the likelihood that the identity represents the presenter, for granting access to requested assets and information.

What's New? Expected Contribution

What makes a specific type of identity document credible? Conversely, how can we recognize potential identity document-related fraud more easily? For example, when someone presents an identity document to open a new bank account, it would be helpful to understand what credibility indicators to focus on, to avoid being deceived by fraudulent identity document types. This could be used as the basis for creating a tool to estimate identity fraud risk associated with the identity document types reviewed. More specifically, the research contribution is:
a methodology to elicit critical attributes in experts' evaluation of the credibility of documentary evidence … applied in the identity fraud domain … resulting in the inter-organizational synthesis of knowledge of the critical credibility attributes elicited.

Success Test? Experts Evaluation

The Repertory Grid Analysis methodology is used to elicit and describe constructs (characteristics) of credibility used by experts, developed by these experts through a process of semi-structured interviews. The participants are given a composite list of the characteristics of

credibility for their validation, then asked to provide, based on their knowledge and experience, their evaluation of these credibility characteristics under four different scenarios.

IV. IDENTITY FRAUD

"*But he that filches from me my good name/*
Robs me of that which not enriches him/
And makes me poor indeed."
(Shakespeare, Othello, Act iii. Sc. 3.)

Perhaps in the 17th century when Shakespeare wrote these lines, it was true to say that stealing my good name "Robs me of that *which not enriches him*," but not so today, with identity theft one of the fastest growing crimes in the USA, enriching the perpetrator at the expense of the victim. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception. (United States Department of Justice, 2007) Typically, the crime is committed for economic gain, although there may be other motivations, such as health care, employment, citizenship, or even terrorism. For example, the Consumer Measures Committee in Canada notes, "It is important to remember identity theft is not always committed for its own sake (...) identity theft is commonly committed to further other criminal activity, such as organized crime and terrorism. Reducing incidences of identity theft may therefore help to reduce broader social harms, such as threats to national security." (Canadian Consumer Measures Committee, 2005)

Types of Identity Fraud

Financial identity theft. This occurs when a perpetrator uses personal information such as a Social Security Number and date of birth to gain financial benefits; for example, opening a

new credit card account. It is important to distinguish between financial identity theft committed on an existing account versus a new account (Howard, 2005). Although these related crimes are often discussed interchangeably, so-called "true name fraud", which occurs when a thief "us[es] a victim's identifying information to open new accounts in the victim's name" (Towle, 2004). This takes a greater toll on its victims than does existing account theft. The financial losses are more substantial, more difficult to discover, and take considerably longer to resolve (Lee, 2003).

Medical identity theft. This occurs when someone: (a) uses a person's name and other parts of their personal health-related data , such as insurance information, without the person's knowledge or consent, to obtain medical services or goods, or (b) uses the person's identity information to make false claims for medical services or goods. In addition to financial effects such as insurance claims, credit cards, and credit reports, medical identity theft also affects individuals' medical lives and medical records. Perpetrators steal medical identities to obtain medical treatment, or to obtain prescriptions or medical devices for resale (Dixon, 2006) . Medical identity theft often causes erroneous data to be entered into existing medical records, and can include creating fictitious medical records in the victim's name. The end result is that medical identity thieves alter victims' medical files to reflect diseases or medical history that the victim does not have.

Homeland Security. The use of fraudulent documents by aliens is extensive, according to officials in the former (pre-2003) Immigration and Naturalization Service (INS-now a section of the Department of Homeland Security). At ports of entry, INS inspectors have intercepted tens of thousands of fraudulent documents in each of the last few years. These documents were presented by aliens attempting to enter the United States to seek employment or obtain other immigration benefits, such as naturalization or permanent residency status (GAO, 2002a). In addition, according to State Department's Bureau of Diplomatic Security Documents, passport

fraud is often committed in connection with other crimes, including narcotics trafficking, organized crime, money laundering, and alien smuggling. Diplomatic Security officials cite concerns that exist within the law enforcement and intelligence communities, that identity theft related to passport fraud could be used to help facilitate acts of terrorism (GAO, 2005).

Business Identity Theft. Personal identity theft is unauthorized use of another person's personal identifying information to obtain credit, goods, services, money, or property, or to commit a felony or misdemeanor. Similarly, business identity theft is the unauthorized use of a business identifying information for the same purpose. "Business identifying information" means a business's name, address, telephone number, corporate credit cards, banking account numbers, federal employer identification number (FEIN), Treasury Number (TR), electronic filing identification number (EFIN; Internal Revenue Service), electronic transmitter identification number (ETIN; Internal Revenue Service), e-business websites, URL addresses, and e-mail addresses (Collins, 2003).

Extent and Characteristics of Identity Fraud

The Identity Relation. An identity is a set of characteristic elements that distinguishes one person from another (Donath, 1999) . Recall that personal identity is a relationship between an individual and an organization. Typically, the organization has custody of certain assets belonging to the individual; for example, a bank may keep the individual's investments, or the individual may have certain rights or privileges to use organizational resources -- for instance, the individual may be an employee, customer, supplier, owner, or a member of a professional association. In any event, the organization issues an identity token to the individual, and keeps a register updated with the issued tokens, so that later on, the individual can claim the assets or other affordances, and the organization can authenticate the claimant, to be sure that the correct

individual receives the correct affordances. Some examples follow of this relation between identity document and organization, viz:

Voter registration card – county electorate roll

Birth certificate – registry of births and deaths

Passport number – State Department

Drivers license – Department Of Motor Vehicles

Student/faculty ID – university

Customer number – pharmacy

Frequent flyer membership – airline

Credit card – credit card company

Measurement. Earliest investigations of the topic by the U. S. General Accounting Office (GAO) discovered that there were no comprehensive or centralized national data, collected by any public or private organization, on the problem of identity theft **(GAO, 2002a**, **b**, **c**, **d)**. Instead, the GAO relied on indicators from various public and private data sources, often gathered specifically at GAO request, and so not necessarily inclusive of all organizations that could be affected by identity theft.

Recall from the identity theft cycle, ABCs of identity fraud, that the C=conversion phase typically facilitates other crimes -- such as money-laundering, alien smuggling and terrorism. Reports of these related crimes do not always isolate the specific identity theft elements of such crimes. For example, "the Federal Reserve Board reported that … fraud involving [the] use of sensitive identifying information is often not tracked separately from other types of fraud" (GAO, 1998). Thus, "the extent of identity theft can be obscured when it is not treated as a separate crime," (Willox Jr., Gordon, Regan, Rebovich, and Gordon, 2004) or overstated if it is treated as synonymous with other fraud crimes. Another measurement difficulty arises because of the lack

of a consistent definition of identity fraud. Many public and private agencies use different indicators of the problem, so that even when data are available, they may not be comparable.

Data are also affected by agency-related variables like policy, staffing, resources, problem awareness, and responses. For example, an apparent decrease of identity theft cases closed by the Secret Service between 1998 and 2000 was due to its decision to focus efforts on high-value cases of identity theft. This decrease was offset by an increase in the average amount of prevented fraud losses for this period (GAO, 2002b). Similarly, one consumer reporting agency attributes increases in consumer inquiries not only to increasing occurrences of identity fraud, but to company growth and consumer outreach efforts; one payment card association attributes a decline in fraud losses between 1996 and 1997 to its antifraud efforts (GAO, 1998).

Identity theft may be underreported, both by individuals and by organizations, as many victims may never discover the crime. The "filched good name" may be both statistically and geographically separated from the real one, especially for the previously described "true name fraud," where personal information is used to open new accounts. Victims may eventually become aware of the crime, but the identity theft may remain undetected for a long time.

Size and Cost of the Problem. In the USA, the number of adult victims of identity fraud has declined marginally between 2003 and 2006, from 10.1 million people to 8.9 million people; the average fraud amount per case has increased from $5,249 to $6,383; and the total one-year cost of identity fraud in the United States has remained relatively flat, increasing from $53.2 billion to $56.6 billion. The vast majority of identity fraud victims (68%) incur no out-of-pocket expenses, and victims are spending more time to resolve identity fraud cases, which has increased on the average from 33 hours in 2003 to 40 hours in 2006 (Better Business Bureau, 2006).

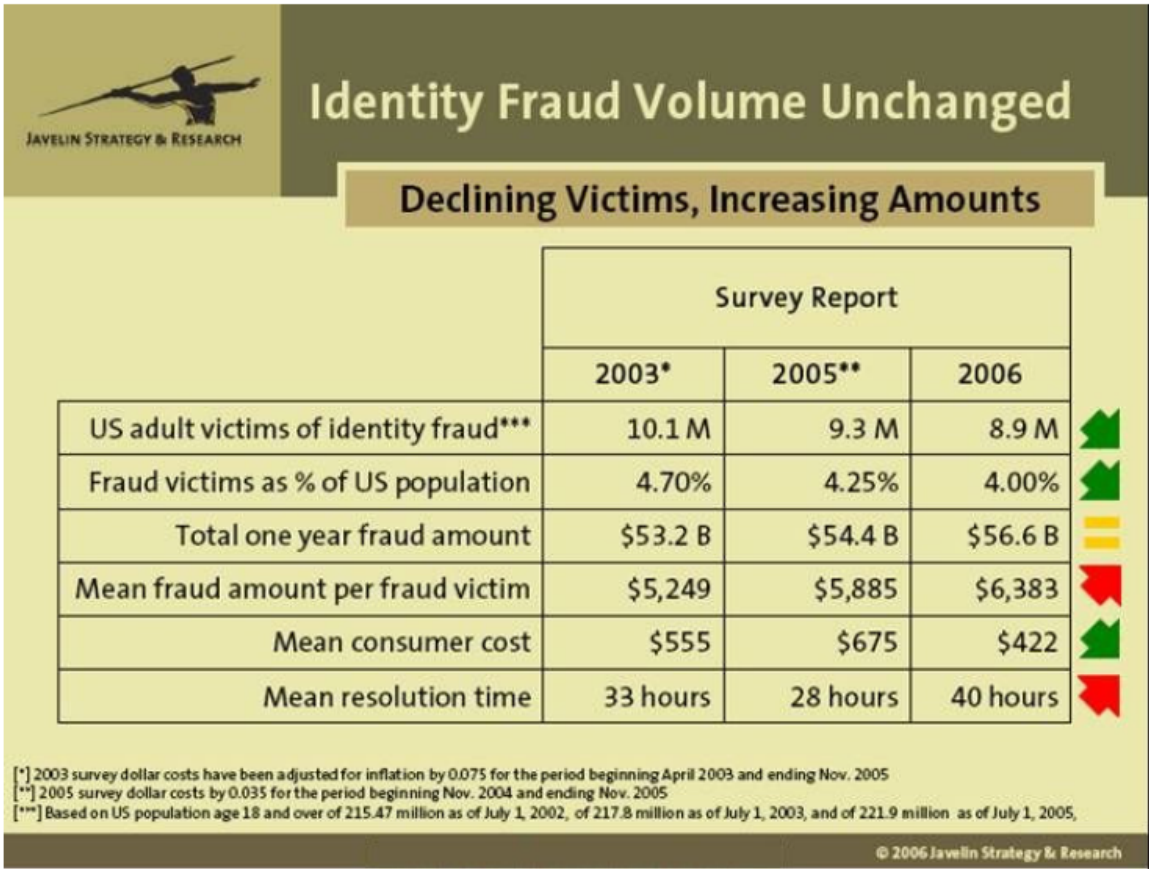

Figure 2. Identity Fraud Volume in 2006

The BBB report is based on a survey by Javelin Strategy and Research, one that includes the graphic at Figure 2. This survey was updated in 2007 (Javelin, S. R., 2007) to show that 8.4 million Americans became the victims of identity fraud, half a million fewer victims than the year before. The total fraud amount dropped 12%, from $56.6 billion to $49.3 billion. The average victim of an existing account fraud paid $587 out-of-pocket in consumer costs. If the thief opened a new account in the victim's name, the average consumer had to pay $617.

The United Kingdom shows comparable results (Bowron and Shaw, 2007). From statistics published in February 2006, the UK economy suffered a financial loss of £1.7 billion

per year from identity fraud, a significant increase over previous years. In 2002, the Cabinet Office reported a loss of £1.3 billion per year.

The "A" in Identity Fraud - Acquisition

The President's Identity Theft Task Force (Gonzales, 2007) lists the techniques most frequently used by identity thieves to steal the personal information of their victims.

Common theft and "dumpster diving" (Mihm, 2003)- While often considered a "high tech" crime, data theft often is no more sophisticated than stealing paper documents from mail boxes, trash receptacles (hence the "dumpster-diving" description), and purse snatchings.

Employee/Insider theft - dishonest insiders can steal sensitive consumer data by removing paper documents from a work site or accessing electronic records. Criminals may bribe insiders, or become employees themselves to access sensitive data at companies.

Electronic intrusions or "hacking" - to steal information from public and private institutions, including large corporate databases and residential wireless networks. Hackers can intercept data during transmission, such as when a retailer sends payment card information to a card processor. Hackers have developed tools to penetrate firewalls, use automated processes to search for account data or other personal information, export the data, and hide their tracks (CERT, 2002). Hackers also can gain access to underlying applications—programs used to "communicate" between Internet users and a company's internal databases, such as programs to retrieve product information.

Social Engineering: "Phishing", Malware/Spyware, and Pretexting - Identity thieves use trickery to obtain personal information from unwitting sources, including from the victim. This type of deception is known as "social engineering." Phishers send emails that appear to be

coming from legitimate, well-known sources, telling the recipient to verify personal information for an account or other service to remain active. The emails provide a link, which goes to a website that appears legitimate, where the web user is instructed to enter personal identifying information, such as his name, address, account number, PIN, and SSN. A new form, dubbed "vishing," (ConsumerAffairs.com, 2006) is where the thieves use Voice-Over-Internet-Protocol (VOIP) technology to spoof the telephone call systems of financial institutions, and request callers provide their account information. Criminals also can use malware/spyware to gain illegal access to Internet users' computers and data without the users' permission. One email-based form of this type of social engineering is the use of emails offering enticing images to victims; by opening the email, the victim launches the installation of malware, such as spyware or keystroke loggers, onto his computer. Pretexters contact a financial institution or telephone company, impersonating a legitimate customer, and request that customer's account information, or it may be accomplished by an insider at the financial institution, or by fraudulently opening an online account in the customer's name.

Stolen Media - criminals steal data storage devices, such as laptops or portable media that contain personal information. Although the hardware may be targeted, the criminal may discover the stored personal information and realize its value and possibility for exploitation.

Failure to "Know Your Customer" - Data brokers gather consumer information from many public and private sources and then offer it for sale to different entities for a range of purposes. For example, government agencies often purchase consumer information from data brokers to locate witnesses or beneficiaries, or for law enforcement purposes. Identity thieves, however, can steal personal information from data brokers who fail to ensure that their customers have a legitimate need for the data. Case in point: In January 2006, the FTC settled a lawsuit against data broker ChoicePoint, Inc., alleging that it violated federal statutes as it failed to

perform due diligence in evaluating and approving new customers. The FTC alleged that ChoicePoint approved as customers for its consumer reports, identity thieves who lied about their credentials, and whose applications should have raised obvious red flags. ChoicePoint paid $10 million in civil penalties, and $5 million in consumer redress and agreed: (1) to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, (2) to establish a comprehensive information security program, and (3) to have audits by an independent security professional every other year until 2026.

"Skimming" - over the past several years, law enforcement authorities have witnessed a substantial increase in the use of devices known as "skimmers." A skimmer is an inexpensive electronic device with a slot through which a person passes or "skims" a credit or debit card. Similar to the device legitimate businesses use in processing customer card payments, the skimmer reads and records the magnetically encoded data on the magnetic stripe on the back of the card. That data then can be downloaded either to make fraudulent copies of real cards, or to make purchases when the card is not required, such as online.

The "B" in Identity Fraud - Breeding New Identity Documents

Thieves often open new credit, utility, or other accounts in the victim's name, make a few charges haphazardly and indiscriminately, and then vanish. Victims often do not learn of the fraud until they are contacted by a debt collector or are turned down for a loan, a job, or other benefit because of a negative credit rating. While this is a less prevalent form of fraud, it causes more financial harm, is less likely to be discovered quickly by its victims, and requires the most time for recovery. When criminals establish new credit card accounts in other names, the whole point is to make maximum use of available credit from those accounts, whether in the short term or long term. Alternatively, new identity documents may not be immediately used for financial

gain. Instead, the thief may use the acquired identity data set to breed other documents such as a driver's license. Breeding continues, to obtain a birth certificate, social security card, and other documents that do not represent the applicant. This in turn provides additional data for the stolen identity document, like parents names, place of birth, etc. Other fraudulent identity documents can be purchased on the "black market."

The "C" in Identity Fraud - Conversion for Financial or Other Gain

The most common form of conversion is misuse of existing accounts such as credit, brokerage, banking, or utility accounts. With credit accounts, for example, the identity thief obtains either the actual credit card, the numbers associated with the account, or the information derived from the magnetic strip on the back of the card. Because it is possible to make charges through remote purchases, such as online sales or by telephone, identity thieves are often able to commit fraud even as the card remains in the consumer's wallet. Recent complaint data also suggest an increasing number of incidents involving unauthorized access to funds in victims' bank accounts, referred to as "account takeovers"

"Brokering" of Stolen Data - marketing of personal identification data from compromised accounts by criminal data brokers. For example, certain websites, known as "carding sites," traffic in large quantities of stolen credit-card data. The Secret Service calculated that the two largest current carding sites collectively have nearly 20,000 member accounts.

Immigration fraud - illegal immigrants use fraudulently obtained social security numbers or passports to obtain employment and assimilate into society. In extreme cases, one social security number may be passed on and used by many illegal immigrants (Leland, 2006).

As previously noted, medical identity theft is the use of a victim's identifying information to obtain or make false claims for medical care (Dixon, 2006). In addition to the financial harm associated with other types of identity theft, victims of medical identity theft may have their health endangered by inaccurate entries in their medical records, as it can cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs. Victims may be unaware of the theft as it can be difficult to discover. Few consumers regularly review their medical records, and victims may not realize that they have been victimized until they receive collection notices, or attempt to seek medical care themselves, only then to discover that they have reached coverage limits, or have some kind of anomalous data in their records.

Law Enforcement Responses to Identity Fraud

Recognizing the Victim. Identity theft affects two victims: the individual whose identity was stolen and the business whose product or service was stolen (Foley and Foley, 2003), and there is anecdotal evidence that corporations are victimized in the same way as individuals (Sullivan, 2004). This is an "equal opportunity crime" (Joint hearing before Subcommittee on Oversight and Investigations 2002). The Foundation for Taxpayer and Consumer Rights in California, reports that "it was able to purchase the Social Security numbers and home addresses for Central Intelligence Agency Director George Tenet; Attorney General John Ashcroft; Karl Rove, President Bush's chief political advisor; and other top administration officials" for $26 dollars each (Swartz, 2003). Similarly, in 2001, a New York City dishwasher used the Internet to defraud millions of dollars from U.S. celebrities and millionaires, including Steven Spielberg, George Soros, and Ross Perot (Barrett, 2002). In another case of more than 100 high-ranking

military officials, the offender was caught with a laptop containing several thousand military names, social security numbers and other types of personal information (Rusch, 2001).

Children represent another type of victim often not recognized. A data source regarding victims under the age of 18 is the Consumer Sentinel Network, but the data are not publicly available in disaggregated form, so the distribution of victimization across the under-18s is unknown; and the deceased have also "long been recognized as favorite targets of identity thieves" (O'Brien, 2004). Of the child victims whose ages were reported to the Sentinel, there were 9,370 victims in 2004 who were under the age of 18 (4% of 234,263); 5,924 in 2003 (3% of 197,475); and 2,618 in 2002 (2% of 130,917). The Identity Theft Resource Center also reports dealing with 2 or 3 new child cases per week, which represents a minimum of 104-156 child victims per year (Davis, K., 2004). Finally, the elderly are also "less likely to engage in credit dependent transactions on a frequent basis and therefore are less likely to become immediately aware that they are victims of an identity thief" (Florida, 2002).

Crossing Jurisdictions: Federal and Local. Identity theft offers perpetrators the advantage of physical distance, and so creates a disadvantage to both victims and authorities. Jurisdictional issues complicate the reporting, investigation and prosecution of identity theft cases, as well as the creation and effectiveness of related legislation. In particular, "the prevalence of identity theft and the frequently multi- or cross-jurisdictional nature of such crime underscore the importance of having means for promoting cooperation or coordination among federal, state, and local law enforcement agencies" (GAO, 2002c). Cooperative efforts falling somewhat outside the realm of the U.S. government have also been created: e.g., (Fisher, D., 2003; Vijayan, 2003) the Coalition on Online Identity Theft, which includes companies such as Microsoft Corp., eBay Inc., Amazon.com Inc., the Business Software Alliance, Network Associates Inc.'s McAfee Security division, and Cyveillance Inc., adopted a four-pronged

strategy to combat online identity theft:

- Promote technology to deal with the problem;
- Expand public education campaigns;
- Share information about emerging fraudulent activities to mprove detection and response, and
- Work with government to ensure stronger penalties for cyber-thieves.

Selected Legislative Responses to Identity fraud

A useful online resource is Law and Technology Resources for Legal Professionals (llrx.com) for following up on the constant legislative and regulatory developments related to identity fraud. "Researching the topic can be a daunting task. Indeed, the recent proliferation of materials, along with the fact that case law is growing exponentially, means that there is a rather large body of literature. In addition, the actual act of identity theft is dynamic and constantly evolving, thus any technical materials are being continually revised." (Paul, 2007)

(Identity Theft and Assumption Deterrence Act 1998) - This was the first piece of federal legislation specifically aimed at identity theft. For the first time, ID Theft became a named federal crime, making it somewhat easier for law enforcement to prosecute. The Act established the Federal Trade Commission (FTC) as the government entity charged with establishing "procedures to ... log and acknowledge the receipt of complaints by individuals", as well as educate and assist potential victims. The term "means of identification" is described as a person's "name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." (U.S.C. § 1028(d)(7)).

(The Fair and Accurate Credit Transactions Act, 2003) - Section 5 addresses identity theft and related consumer issues. Victims of identity theft are granted the ability to work with

creditors and credit bureaus to remove negative information in their credit report resulting from identity theft. FACTA also created requirements to prevent identity theft, such as requiring merchants to truncate credit card numbers on receipts, and enabling consumers to request that a credit bureau truncate their Social Security number when disclosing their credit report (15 U.S.C. § 1681g(a)(1)(A)). Individuals can also order a copy of their credit report free of charge once every year (15 U.S.C. § 1681j).

(Wang, G., Chen, and Atabakhsh, 2004) - This statute established penalties for aggravated identity theft. This includes instances when identity theft has been used as the first step in a process of more serious crimes, such as terrorist acts, immigration violations, and firearms offenses. The Act directs the U.S. Sentencing Commission to amend the Federal sentencing guidelines so that individuals who gain access to the information used to commit identity theft at their place of employment face increased penalties.

(Internet False Identification Act 2000) - This statute addresses computer-aided false identity crimes. It expanded the scope of the fraudulent identification document crime to include document transfer by electronic means, with the intent to end the distribution of counterfeit identification documents over the web. According to the FDIC, the Act closed “a loophole left by the ID Theft Act, [enabling] law enforcement agencies to pursue those who formerly could sell counterfeit social security cards legally by maintaining the fiction that such cards were "novelties" rather than counterfeit documents” (Federal Deposit Insurance Corporation, 2004). As a result, the statute now accounts for computer-facilitated crimes of false identity and prohibits possession, production, or transfer of false identification documents or identification documents that were not legally issued to the possessor (18 U.S.C. §§1028 (a)(1), (2)). It also prohibits the production, transfer, or possession of any "document making implement" that is intended for use in manufacturing false identification documents (18 U.S.C. §§1028 (a)(5)).

(Social Security Number Confidentiality Act 2000) - prohibits displaying social security numbers on unopened checks or other Treasury issued drafts.

Ongoing Identity Fraud Research

An excellent summary (Figure 3) of ongoing research efforts to reduce identity theft is provided by (Newman and McNally, 2005) In addition, a variety of approaches has been taken to identify the identity fraud problem.

Data Mining. Typically, these are transaction-oriented methods, where individual financial transactions are collected and analyzed for unusual activity. Many of us for example may have experienced receiving a telephone call if we use a credit card in a strange city or country, or for an unusually large amount. The transaction shows up as unusual, and so the merchant is alerted to perform some kind of additional verification, or perhaps the credit card company requires direct conversation with the customer. Another application of the data mining approach is described (Zdanowicz, 2004) where data mining techniques are applied to financial transactions to estimate money laundering and terrorist financing based on the analysis of historical price data of US imports and exports. Analysis can be conducted in real time to determine which transactions should be audited and which cargo shipments should be inspected.

TABLE 2: TECHNIQUES TO REDUCE IDENTITY THEFT

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
Target harden ▪ Tamper proof credit cards ▪ Firewalls ▪ Tamper proof ID documents ▪ Shred utility bills etc. *Control access to facilities* ▪ Lock mail boxes ▪ Card/password access to ID databases ▪ ID for mail forwarding ▪ Disallow remote access to databases ▪ Limit number of persons with access to ID databases *Deflect offenders* ▪ Require several forms of ID to obtain new ID or replacement. *Control tools/ weapons* ▪ Control sale of ID making equipment (card readers, stripers, printers) ▪ Use tracking ID tags to track location of use and who uses machine	*Extend guardianship* ▪ Close scrutiny, background checks of employees with access to ID databases *Assist natural surveillance* ▪ ATMs in well lit areas ▪ Disallow employees to take work home ▪ Support whistleblowers *Reduce anonymity* ▪ Photo, thumb print on ID documents, credit cards ▪ Require additional ID for on-line purchases ▪ Train clerks, police, officials in document authentication procedures *Utilize place managers* ▪ Reward vigilance for supervisors of employee/customer records *Strengthen formal surveillance* ▪ Retain backup files of computer usage ▪ Track keystrokes of computer users ▪ Monitor all utilization of ID databases ▪ Cameras on ATMs, at check-out counters, shipping and mailing services, ID granting agencies ▪ Background checks of employees	*Conceal targets* ▪ No social security numbers on health, school cards ▪ No credit card numbers on receipts ▪ Place ATMs so keystrokes cannot be observed or recorded ▪ Shred utility bills *Remove targets* ▪ Pre-paid cards for pay phones ▪ Smart cards that contain limited personal ID information ▪ Do not leave wallets in cars *Identify property* ▪ Guaranteed ID authentication services (e.g. Microsoft Passport) ▪ Vehicle ID licensing and parts marking *Disrupt markets* ▪ Monitor pawn shops ▪ Monitor retail returns departments ▪ Monitor deliveries to vacant houses ▪ Monitor classified ads. *Deny benefits* ▪ Swift notification of stolen credit card	*Avoid disputes* ▪ Maintain positive management-employee relations *Reduce arousal and temptation* ▪ Avoid public disclosure of security holes and patches in software ▪ Do not boast of security features in software	*Set rules* ▪ Responsible computer use policy *Post instructions in college dorms, workplace* ▪ "Respect Privacy" ▪ "Protect our customers' privacy" *Alert conscience* ▪ "Hacking hurts people" Assist compliance ▪ Provide shredders for employees

Adapted from Clarke and Eck (2004) and Clarke (2004).

Figure 3. Techniques to Reduce Identity Theft

Risk Factor Analysis. This approach is exemplified by the consumer credit score approach taken by the companies that provide credit-checking services. The most common overall measure of personal credit is the FICO score, used by most lenders to determine personal credit risk. There are three FICO scores, one for each of the three credit bureaus – Experian, TransUnion, and Equifax – and each of these scores is based on information the credit bureau keeps on file. As personal information changes, so does the credit score. The calculation is based primarily on five major credit risk categories. The first category is a detailed payment history of items, and your habits of making payments in full and on time. The second is the amount of outstanding credit, overall and by account. Third is the length of credit history, showing the amounts of time since accounts were originally opened, and since the last activity. Fourth is the types of credit used -- mortgage loan is considered lower risk than retail credit, for example. Finally, the fifth risk factor considered is new credit accounts: the lines of credit recently established -- how much is used on each line, any past problems, and so on.

V. CREDIBILITY

Credibility has been researched in multiple domains ranging from communication, information science, psychology, marketing, and the management sciences to interdisciplinary efforts in human-computer interaction (HCI). Each domain examines the concept and its practical significance using fundamentally different approaches, goals, and presuppositions, which results in conflicting views of credibility and its constructs.

Disciplinary approaches to investigating credibility systematically developed only in the last century, beginning within the field of communication. Seminal among these efforts was (Hovland, Janis, and Kelley, 1953; Hovland and Weiss, 1951), who focused on the influence of various characteristics of a *source* on a recipient's message acceptance. This work was followed

by many years of research on the relative credibility of *media* involving comparisons between newspapers, radio, television, and the Internet (Meyer, 1988; Newhagen and Nass, 1989; Quinn, 2004; Slater and Rouner, 1996). Historically, communication researchers have focused on sources and media, viewing credibility as a *perceived characteristic*. In the information science domain, the focus is on the evaluation of *information*, most typically instantiated in documents like identity tokens, and statements like those claiming to be the person represented by the token. In these situations, credibility has been viewed mostly as a criterion for relevance judgment (Barry, C. L., 1994; Bateman, 1998; Cool, Belkin, and Kantor, 1993; Schamber and Bateman, 1996; Wang, P. and Domas-White, 1999), with researchers focusing on how information seekers assess a document's likely level of quality (Liu, 2004; Rieh, 2002).

Concepts Related to Credibility

Persuasiveness. The working definition for credibility actually has ancient origins. Aristotle, writing in the 5th century BC, discussed the notion of credibility in his examination of *ethos*, as he relates it to his observations of speakers' abilities to persuade listeners to believe them. (Aristotle, 1991 translation). This view is retained today — Webster's New World Dictionary defines credibility as believability. Credible people are believable people; credible information is believable information (Fogg, Swani, Treinen, Marshall, Laraki, Osipovich, Varma, Fang, Paul, and Rangnekar, 2001). Aristotle's idea of "persuasion through character" captures many of the underlying assumptions that are now influential in credibility research in general. The concept supports this research; recall that the definition for credibility of an identity document is the likelihood that the identity document represents an individual, for the purpose of granting access to requested assets and information.

Source, Message, Media. Credibility is frequently attached to objects of assessment, as in *source credibility*, *media credibility*, and *message credibility*, reflecting the fact that assessments of these objects differ (Kiousis, 2001). Credibility assessments of sources and messages are fundamentally interlinked and influence one another (Slater and Rouner, 1996) — credible sources produce credible messages and credible messages come from credible sources (Fragale and Heath, 2004). Roper Research Associates for the Television Information Office used the approach of asking the question: "If you got conflicting or different reports of the same news story from radio, television, magazines, and newspaper, which of the four versions would you be most inclined to believe?" (Roper, 1985). This sought to discover perceptions of the *relative credibility* of different news media. However, it was not helpful in getting toward the goal of this current research -- to identify and measure the attributes of credibility, see (Nass and Mason, 1990), for a general critique), -- or the processes used in evaluating different types of media, or what characteristics of a medium influence credibility assessments (Burbules, 2001).

Trust and Belief. Trust has been a core construct in many early and more recent conceptualizations of credibility (Hovland, Janis, and Kelley, 1953; Marsh and Dibben, 2003);. Providing a good overview of the theoretical meanings of trust, these researchers argue that trustworthy interfaces become enabling technologies because they lead the user to want to interact with them, thus increasing productivity. Other researchers (Tseng and Fogg, 1999) point out that, although credibility and trust have sometimes been used interchangeably, they should not be considered synonymous. Trust is different from credibility because "trust indicates a positive belief about the perceived reliability of, dependability of, and confidence in a person, object, or process". They suggest that, in the field of HCI, trust refers to dependability and credibility is roughly synonymous with believability. Trust frequently refers to a set of beliefs, dispositions, and behaviors associated with the acceptance of risk and vulnerability. Credibility

refers to a perceived quality of a source, which may or may not result in associated trusting behaviors.

Quality and Authority. In his conceptual model of information quality (Taylor, 1986) identified six categories of user criteria for making choices: ease of use, noise reduction, *quality*, adaptability, time saving, and cost saving. He defined quality as "a user criterion which has to do with excellence or in some cases truthfulness in labeling" and identified five values included in quality: accuracy, comprehensiveness, currency, reliability, and validity (p. 62). Although Taylor did not explicitly use the term "credibility," the notion seems to be embedded in his derivation of quality from reliability and validity. The theory of cognitive authority (Wilson, 1983) is closely related to the concept of credibility. Both feature trustworthiness and competence as their main components. Only those who are deemed to "know what they are talking about" are recognized as cognitive authorities. Wilson claims that people do not attribute cognitive authority exclusively to individuals. Cognitive authority is also found in books, instruments, organizations, and institutions. Wilson points out that an authority's influence on us is thought proper because "he is thought credible, worthy of belief"

Expertise. Expert systems are generally viewed as credible advisers in a wide range of domains and circumstances, even though such systems use static information and rules applied to dynamic problems. (Dijkstra, 1999) as well as (Murphy, 1996) have shown that when users cannot verify information from expert systems, they rely on other cues -- such as the degree to which the interaction with the system is enjoyable -- in deciding whether to accept the system's output. This is similar to social interactions, where source credibility is often relied upon in place of a more rigorous examination of claims and arguments (Petty and Cacioppo, 1986). Some researchers (Wærn and Ramberg, 1996) have tried to compare responses to advice from expert systems (and other information systems) to human advice. They found that users perceive human

and computer advisers differently, but do not always perceive or respond differently to the advice. There seems to be no differences between the perception of advice given by computers and by people, but there is some evidence that humans and computers may be perceived as more or less trustworthy according to the task. (Dijkstra, Liebrand, and Timminga, 1998) found similarly that users perceive expert systems as more objective than humans. (Lerch, Prietula, and Kulik, 1997) found that users place greater confidence in human advice than in advice provided by an expert system.

Contexts Affect Credibility Constructs

World Wide Web. The issue of credibility has been investigated most thoroughly at this level of analysis. Here, the individual Web site has been viewed as the source; credibility in this context is often referred to as Web site credibility. Users perceptions of credibility have been conceptualized along three dimensions (Flanagin and Metzger, 2003): (1) message credibility (i.e., the perceived credibility of the information residing on a Web site); (2) sponsor credibility (i.e., the perceived credibility of the individual whose site is represented); and (3) site credibility (i.e., the perceived credibility of the Web site as a whole). In other related research, (Abels, White, and Hahn, 1997) collected data from faculty members by asking them to engage in "brainwriting" during a focus group conducted in an electronic environment. The six clusters that reportedly influenced the use of Web sites were appearance, content, linkage, special features, structure, and use. These authors noted that "when a user states that information must be useful, they are referring not only to topic coverage but also to the source or producer of the information" (White, Abels, and Hahn, 1998). Fogg and other members of the Stanford Web Credibility Research project conducted many studies on Web site credibility issues. These include (Fogg,

2003; Fogg, Marshall, Kameda, Solomon, Rangnekar, Boyd, and Brown, 2001; Fogg, Swani, Treinen, Marshall, Laraki, Osipovich, Varma, Fang, Paul, and Rangnekar, 2001) and others.

Relevance Judgments. Information science researchers have considered assessment of credibility to be part of relevance judgments. In the 1990s, several empirical studies (Barry, C. L., 1994; Cool, Belkin, and Kantor, 1993; Park, 1992; Peiling Wang, 1998; Wang, P. and Domas-White, 1999) were conducted to identify user-defined relevance criteria. These studies revealed that people use much more diverse criteria than mere topicality for their relevance judgments. Interestingly, user-defined relevance criteria show common characteristics and factors across studies conducted in meteorology, health, and scholarly information (Barry, C. and Schamber, 1998; Wang, P., 1997). The findings of eleven previous studies on relevance criteria were compared (Maglaughlin and Sonnenwald, 2002), counting the number of times each criterion was identified. Relevance criteria that appeared consistently and often, included subject matter/topic, authority, completeness/depth, currency/recency, accuracy/quality, affectiveness, belief, credibility, clarity, and document type. It should also be noted that information science researchers often use the broader term quality to denote the concept of credibility. For instance, (Barry, C. L., 1994) found that academic users employed criteria pertaining to evaluation of a document's source in terms of source quality and source reputation/visibility. Other research work (Wang, P. and Soergel, 1998), (p. 120) revealed the criterion of "expected quality," which is defined as an estimation of the goodness of a document in terms of journal quality and author quality. Information credibility has been researched in the context of information seeking (Bateman, 1998). In a survey of more than 200 graduate students, she identified the eleven most important criteria and used a factor analysis to develop a three-dimensional model of relevance: information quality, information credibility, and information completeness. These three factors explained 48% of the respondents' concepts of relevance. Bateman's studies indicate that quality and credibility were very important to her user group. Users wanted information that was not

only accurate, credible, well written, focused, understandable, and consistent; but also easy to obtain, current, and on their topic. This suggests that the research in this dissertation is generalizable.

Information Seeking and Retrieval. Relevance has been considered the primary criterion in selecting information (Saracevic, 1996; Stefano, 1997), and in fact the term "credibility" did not appear in literature on information seeking and retrieval until the 1990s (Fritch and Cromwell, 2001; Janes and Rosenfeld, 1996; Wathen and Burkell, 2002; Watson, 1998). Also, research published by (Olaisen, 1990) addressed the authority and credibility of electronic information, finding that the "knowledgeable person" was the most important source for both daily administrative decisions and strategic long-term decisions; these sources ranked high in credibility, influence, reliability, and relevance. Electronic information was emerging as an important source, scoring highly in relevance, perceived value, accessibility, actual value, flexibility, and browsing possibilities, but low in credibility, form, and user friendliness. Rieh examined the problems of information quality and authority in Web searching by identifying the factors influencing people's judgments of information (Rieh, 2000, 2002; Rieh and Belkin, 1998). The Web users in Rieh's studies paid considerable attention to institutional authority, giving greater credence to academic and governmental institutions. They also took into account the affiliation of the author/creator, assigning higher levels of authority to professional experts such as professors, doctors, and librarians.

Explanation, Claim, or Verification. It is important to understand perceptions of individuals who make decisions about whether to accept identity documents. Do the documents provide an explanation of the holder's privileges, or a claim to the affordances provided by the organization, or simply verification of some inherent holder characteristic? This affects the

dimensions of credibility considered important for this research. For the future, it may also suggest how a credibility evaluation tool can be designed to make it most effective for the user.

Explanation facilities may be invoked by the user, remain constantly present, or be presented to the user based on an analysis of user interactions with the system (Gregor and Benbasat, 1999). The research tells us that explanations provided by these facilities can vary in both referent and form, with trace or line-of-reasoning explanations providing the logic behind the decision. Justification or support explanations point to extensive reference material in support of a full or partial decision. Control (or "strategic") explanations indicate the problem-solving strategy used in arriving at the conclusion. Finally, terminological explanations provide definition information (Ye and Johnson, 1995). For example, they found that auditors were more likely to accept expert system advice when the system's reasoning process was made clear by explanations, with justification explanations being the most effective.

Factual claims describe objectively verifiable product features such as performance dimensions; evaluative claims appeal to subjective and emotional responses to intangible aspects of the product such as prestige of ownership (Holbrook, 1978). About 15 years later, (Darley and Smith, 1993) separated two critical dimensions of objectivity (factual/impressionistic and tangible/intangible), and showed that maximally objective claims will be factual and will refer to tangible attributes, but that maximally subjective claims will be impressionistic and refer to intangible attributes. Factual claims regarding intangible attributes are argued to be impossible, as is consistent with most conceptualizations of these dimensions (Ford, G. T., Smith, and Swasy, 1990). When source credibility is high, claim extremity is positively related to attitude (Goldberg and Hartwick, 1990).

Verification - if, when, and at what cost - is probably the most critical aspect of product claims with respect to credibility. Subjective claims are inherently less credible; sellers may

exaggerate such claims just enough to entice potential buyers to incur the above costs but not to the degree that discovered exaggeration overwhelms search costs (Nelson, 1974). Experience quality claims, too, differ in typical verification costs. The price of a good is often an immediate roadblock to verification; an inexpensive good may be tried and discarded if it fails to meet a consumer's needs. Even when price does not significantly hinder "trialability" (Rogers, 1995) (p. 243), some product attributes, such as the durability of a running shoe, can be assessed only after a considerable amount of usage (Davis, E., Kay, and Star, 1991). Prior to that, (Darby and Karni, 1973) further distinguished experience qualities that are costly to evaluate from credence; this distinction makes verification costs impossible, for all practical purposes.

Organizational Background and Situational Idiosyncrasies. Some kinds of organizational norms and biases (for example, auditors) may make some types of system recommendations more acceptable than others (Swinney, 1999), leading to over-reliance. If trust in automation is low, operators may consequently view such systems as less credible and thus reject accurate information (Muir, 1987). As early as the 1970s, (Luthans and Koester, 1976) and (Koester and Luthans, 1979) found evidence that experience may influence one's tendency to accept and comply with suggestions from computers. They found that highly experienced users may be overly skeptical and that inexperienced users tend to over-rely on suggestions from computers, as compared to a control condition with mimeographed lists of the same suggestions. This finding fits with an early belief among researchers that users are likely to be "in awe" of computers, viewing them as credible in a wide range of domains (Pancer, 1992), but later experiments show little evidence for this belief (Andrews and Gutkin, 1991; Wærn and Ramberg, 1996).

Evaluating Credibility

Underlying Constructs. Researchers, particularly in interpersonal and mass communication, have long understood credibility to be a multidimensional concept (McCroskey and Young, 1981) but have not always agreed on its underlying dimensions. These include trustworthiness, expertise, dynamism, competence, and goodwill. There are two approaches used widely by researchers to try and distinguish the dimensions of credibility: the *creation* of candidate terms relevant to credibility and the *validation* of these candidate items, resulting in a reduced set indicative of the construct's primary dimensions. In the creation stage, researchers attempt to generate a list of terms that, at face value, are relevant to credibility. For example (Singletary, 1976) and (Vandenbergh, Soley, and Reid, 1981) asked participants in their studies to imagine a specific high-credibility source (in Singletary's case, a news person; in VandenBergh et al.'s, an advertiser) and to list as many terms as possible that, in the participant's view, gave credibility to that source. Other researchers either sampled the existing literature to create a list of candidate terms based upon their review or relied upon intuition. In the validation stage, these candidate terms are summarized and reduced, most often using factor analysis.

Additionally, it is important to recognize that the target of a researcher's interest — be it public speakers, newspapers, Web sites (or identity documents) — likely has a critical impact on the dimensions the researcher uncovers. (Newhagen and Nass, 1989) showed that information seekers use different criteria to evaluate newspapers and television and that this can lead to differences in assessments of both those media, and in conclusions as to the important dimensions of credibility.

Creation methods. The first and most obvious difficulty is in choosing the right approach for generating candidate terms. The validation stage is only as good as the generation stage; if creation methods fail to generate a sufficiently broad range of terms or if the set of terms is itself

biased in some way, the results of the validation stage will be similarly biased. The repertory grid technique used for this stage of the dissertation research has proven very useful in removing these biases. In other approaches, a number of relevance studies, for example, collected user-based criteria simply by asking users what made them think that the information was useful without developing a predefined set of relevance criteria. The user criteria were derived from content analysis of oral or written reports (Barry, C. L., 1994; Cool, Belkin, and Kantor, 1993; Park, 1992; Wang, P. and Soergel, 1998).

Validation methods. One approach for reducing the number of candidate terms has been the use of factor analytic methods. This carries inherent limitations, particularly with respect to the subjectivity of interpreting results (Infante, Parker, Clarke, Wilson, and Nathu, 1983; Meyer, 1988). However, factor labeling is subjective and, so it is often unclear whether dimensions identified by different researchers as representing similar but distinct sets of terms are in fact the same, "expertness" and "competence" being a case in point. Other methodological issues, such as participant response, may be set using semantically different scales and so can influence which dimensions emerge in a given study. Again, the use of the repertory grid technique has the effect of removing the subjectivity of the researcher.

Dimensions versus predictors. Even relatively rigorous creation and validation stages face a fundamental problem: It is often unclear whether the factors identified are mere predictors of source credibility or representative of an underlying dimension of the construct (Newhagen and Nass, 1989). The "face validity" of proposed dimensions is largely subjective; for example, should dimensions referring to extroversion of a communication source be seen as a just a correlate of source credibility, or a distinct dimension (McCroskey and Young, 1981).

Credibility Defined for this Research

This section of the literature review is organized around five ideas.

(1) Credibility is the chief element of information quality composed of situation-dependent dimensions and criteria for evaluation. Researchers in information science have traditionally situated credibility in relation to relevance judgments. Relevance is often defined as users' perceptions of the potential usefulness of information; relevance judgments, as users' decisions to accept or reject specific information items (Schamber and Bateman, 1996). Information quality, credibility, and cognitive authority are those criteria that have appeared consistently across relevance studies (Wang, P., 1997).

(2) Research must be oriented toward the targets of credibility assessment -- the different types of identity documents. In every discipline applying credibility to the use of technology, users tend to respond to information systems as if they were the source of the information being delivered. This is a direct consequence of users' social responses to technology (Reeves and Nass, 1996). Information seekers may be doubtful of a medium, without reference to more specific sources, in the same way they are doubtful of more traditionally recognized sources such as organizations and individuals (Rieh and Belkin, 1998). Just as importantly, information technology presents users with numerous new objects that might be perceived as sources. In many cases, the messenger, by virtue of its virtual proximity to the information seeker, *is* the perceived source.

(3) Credibility assessment processes comprise prediction, evaluation, calibration, and verification. A key distinction in the literature of credibility assessment processes is between two kinds of judgments: predictive judgments made prior to accessing the object of assessment and evaluative judgments made when confronting the object of assessment. The distinction originates

from (Hogarth, 1996) judgment and decision-making theory, and has been most explicitly applied to credibility assessment in information seeking and retrieval.

(4) The situational aspects of credibility assessment are made with respect to domain, user goals, motivation, environmental constraints, and organizational and social contexts. Researchers recognize the importance of the context of credibility assessment, both the relatively idiosyncratic situational variables that can influence judgment, as well as the broader social and organizational background within which assessments are made.

(5) The evaluator's background produces a certain orientation toward new sources and information, evaluative skills, and domain knowledge. Common to all credibility assessment research is the recognition that assessments are made in relation to an evaluator's existing knowledge and beliefs and that this background often drives information-seeking strategies. A second critical aspect of credibility assessment with information technology is the frequent need for users to develop novel evaluative skills. Examining a set of production rules explaining a recommendation by a decision-support system is an indicator of credibility.

The concept of credibility can be applied to identity-related information systems in two ways. The first way is to teach people to evaluate information, so that they obtain it from credible sources: two approaches are the checklist model and the critical thinking model. The checklist model has some limitations because evaluation of information is subjective, relative, and situational, rather than objective, absolute, and universally recognizable. The second way is to design information retrieval systems in which various aspects of credibility judgments can be integrated with topical relevance to improve search performance. Together, they help people secure good, useful, reliable, and trustworthy information to help them with the task at hand.

As an analogy, teaching critical thinking aims to teach students by addressing issues such as how to make a quality assessment when potentially relevant materials have been located

(Cooke, 1999). The criteria proposed tend to be drawn from librarians' experience of selecting materials for their collections. From this analogy, although not all are specific to identity documents, the following items suggested by the literature may be useful (Alexander and Tate, 1999; Dragulanescu, 2002; Kjartansdóttir and Widenius, 1995a, b; Nicolae-George, 2002; Pratt, Flannery, and Perkins, 1996).

- Objectivity issues: Is there a statement of the aims, objectives, and intended coverage presented with a minimum of bias?
- Source reputation issues: What are the reputation and experience of the author or institution responsible for the information?
- Currency and maintenance issues: Is information up-to-date?
- Information accuracy issues: Is the information factually accurate? Are there any typographic, spelling, or grammatical errors?
- Presentation of information issues: Is the information clearly presented and arranged?

VI. CONTRIBUTION

The expected contribution of this dissertation research is to discover/expand a list of the components of credibility that are associated with potentially fraudulent digital identity document types. Based on the literature review, this appears to be the first time the repertory grid technique will be applied to elicit the underlying components of the credibility construct. Most researchers up to now, have used intuition, or based their work on components previously identified in the literature. This will provide a kind of expert opinion on what constitutes credibility, as the repertory grid methodology will be based on a series of structured interviews of the personnel who normally review these types of identity documents and make decisions based on their review.

Additionally, the research will assign measures to each component to develop a composite index of credibility. Four scenarios are presented to participants, to reflect the fact that their evaluation is likely to change with relevant knowledge and experience. This is a unique use of an empirical analysis, based on expert opinion, to validate these components, many of which are not measurable in the usual sense of the word. Furthermore, the method is based on having the experts evaluate the probability that different types of documents are fraudulent, or not. This probability of course is the basis for the decision to grant the requested affordance, or not.

Fraud Potential In Identity Document Types

Modeling Credibility. It has been already established that victims of true-name fraud -- identity theft for new financial accounts -- are most at risk. True name fraud typically causes greater financial loss, is more difficult to discover, and usually takes much longer to resolve. Also, the greatest risk of identity fraud exists at the beginning of the interaction with a financial organization, when an individual is new to the organization, and the organization has had no previous contact with the individual. The combination of identity fraud type and timing provides the focus for this research, as developing a tool to estimate the potential for identity fraud at this high-risk time of new customer authentication is the overarching goal.

This effort is hindered because of the difficulty to observe directly the probability of such fraud. Alternatively, a set of characteristics that can be observed and measured, are used as a metric to find the answer to the research question: what is the potential for fraud in different types of identity document presented when new customers apply to open an account? In other words, measuring credibility of the identity document types is proposed as the metric for fraud potential. This is the specific goal of this research.

The credibility model is shown below. The unit of observation is identity document type. The research objective is to discover the constructs that experts use to think about credibility in identity documents. These constructs are given importance ratings by the experts in each of four different scenarios. Five major steps are developed in the model. The first step is to select domain-representative elements. Second is to elicit the experts' constructs -- the components of credibility. Third, is to construct a set of scenarios that consider the major uncertainties that could affect the context in which identity document credibility could be judged. Fourth, the experts provide, for each scenario, estimated measurements of the importance of each one of the elicited constructs; the characteristics that make identity documents seem credible. This measurement represents expert judgments of the potential for identity fraud. Finally, in step five, the individual expert evaluations are synthesized, to determine if there is some level of consensus.

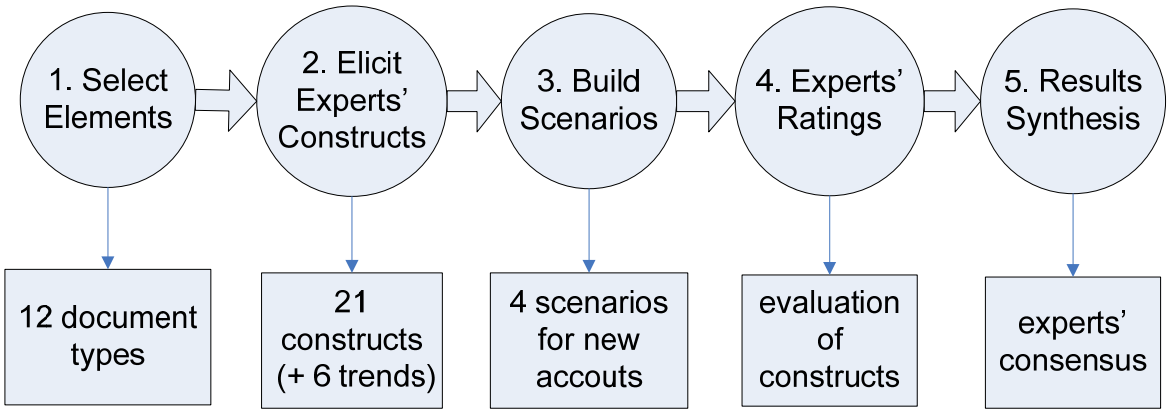

Figure 4. Identity Theft Research Model

Eliciting the Components. Historically among researchers, this process of eliciting the components of credibility has been accomplished in one of three ways: researcher intuition, literature review for terms relevant to the research context, or asking research participants to list

components. However, all these methods are open to bias and subjectivity; a more structured approach is desirable. Such an approach is provided by the repertory grid methodology.

Repertory Grid. The repertory grid technique is "a form of structured interviewing that arrives at a description ... of the interviewee's constructs on a given topic ..." (Fransella and Bannister, 1977; Jankowicz, 2003) such as credibility of IDs. It is proposed for this research to help overcome most of the subjectivity and bias that has hindered prior research related to credibility. These have been discussed throughout the literature review, but the more important ones are summarized here again for emphasis. Labeling of factors carries inherent limitations, particularly with respect to the subjectivity of interpreting results, for example, "expertness" and "competence". Choosing the right approach for generating candidate terms is also a potential problem. If the creation stage of the research fails to generate a sufficiently broad range of terms, or if the set of terms is itself biased in some way, the results of the validation stage will be similarly biased. Participant response options may be set using semantically different scales and so can influence which dimensions emerge in the study. Validity of proposed dimensions is often subjective; for example, should dimensions referring to extroversion of a communication source be seen as a just a correlate of source credibility, or a distinct dimension.

Identifying Trends. During the process of eliciting the characteristics of credibility from the experts, they are also asked to identify trends in industry, technology, globalization, or other arenas, that could be expected to impact their evaluation of credibility in identity documents presented for opening new accounts.

Building Scenarios. These trends are then used to develop scenarios of different future situational contexts in which the evaluation of the identity documents occurs. These different scenarios can be used to establish different base criteria for the credibility index.

Specific Deliverables

Repertory Grid Questionnaires and Construct Analysis. As far as can be discerned from review of the literature, this effort represents a substantial contribution to theory, as it is the first to use the repertory grid technique to elicit the components of credibility of identity documents. In addition, the technique may add to the list of identified components of credibility in the context of fraudulent identity document types.

Scenario Analysis. The scenario analysis provides a general validation of the characteristics identified by the RGI methods, as it provides validation of the relative importance of each characteristic.

VII. METHODOLOGY

Theoretical Perspective

This research borrows from a number of different, but well-established theoretical backgrounds. First, identification of the components of credibility draws upon personal construct psychology (Kelly, G., 1955), the underpinning for the repertory grid technique, "a form of structured interviewing that arrives at a description ... of the interviewee's constructs on a given topic ..." (Fransella and Bannister, 1977; Jankowicz, 2003) such as credibility of identity documents. Second, determining an appropriate classification, ordering, or ratio scale for each credibility component draws on measurement theory (Krantz, Luce, Suppes, and Tversky, 1971; Roberts, 1979) to determine appropriate representation (normative, descriptive, axiomatic) and utility (uniqueness, consistency, additivity). Third, calculating a composite index of these measurements will require application of index number theory (Diewert and Nakamura, 1993; Fisher, I., 1922; Vogt and Barta, 1997).

Personal Construct Psychology. The main tenet of Personal Construct Psychology theory is: A person's unique psychological processes are channelized by the way he anticipates events (Kelly, G. A., 1992). Kelly believed that anticipation and prediction are the main drivers of our mind.

> "*Man is a scientist in that he is always building up and refining theories and models about how the world works so that he can anticipate events. We start on this at birth (if I cry, mommy will come, discovers Baby...), and continue refining our theories as we grow up. We build theories -- often, stereotypes -- about other people and also try to control them or impose on others our own theories so that we are better able to predict their actions.*"

All these theories are built up from a system of constructs. A construct has two extreme points, such as "happy-sad"; we tend to place people at either extreme or at some point in between. Our mind, says Kelly, is filled with these constructs, many of them unconscious. A given person or set of persons, or any event or circumstance, can be characterized fairly precisely by the set of constructs we apply to it and the position of the thing within the range of each construct. Ken, for instance, may be just halfway between happy and sad (one construct) and definitively clever rather than stupid (another construct); whereas Jan may be all the way happy, but of average intelligence, halfway between clever and stupid. A baby may have an unconscious construct "Comes... doesn't come: when I cry". An experienced bank teller looking at a proffered identity document may have an conscious construct "Good-reputation … bad-reputation:" for the known issuer of some kind of identity document.

Constructs apply to anything we pay attention to, including ourselves, and also strongly influence what we fix our attention on. We construe reality by creating constructs. So determining a person's system of constructs would help in understanding that person, especially those essential constructs that represent very strong and unchangeable beliefs (wikipedia.org, 2007a).

Repertory Grid. Kelly believed in a non-invasive approach to psychotherapy. Rather than having the therapist interpret the person's psyche, which would amount to imposing the doctor's constructs on the subject, the therapist should just act as a facilitator of the subject finding his own constructs. The subject's behavior is then mainly explained as ways to selectively observe the world, act upon it and update the construct system in such a way as to increase predictability. To help the subject find his constructs, Kelly developed the Repertory Grid Interview technique. The Repertory Grid is a matrix where rows represent constructs found, columns represent the elements, and cells indicate with a number the position of each element within each construct (Fransella, Bannister, and Bell, 2004).

To build a Repertory Grid (matrix) for a subject, Kelly would first ask the subject to select about seven elements whose nature might depend on whatever the subject or therapist are trying to discover. For instance, "Two specific friends, two work-mates, two people you dislike, your mother and yourself", or something of that sort. Three of the elements would be selected at random, and then the therapist would ask: "In relation to … (whatever is of interest: for example, social compatibility), in which way are two of these people alike, but different from the third"? The answer is sure to indicate one of the extreme points of one of the subject's constructs. He might say for instance that Jack and Jill are very communicative whereas John isn't. Further questioning might reveal the other end of the construct (introvert, perhaps) and the positions of the three characters between extremes. Repeating the procedure with different sets of three elements ends up revealing several constructs for which the subject might not have been fully aware.

Although the grid was developed as an approach to psychotherapy, it is simply a specific format for a structured interview, exploring another person's construct system to understand the way in which the other person views the world, and in what terms the person seeks to assess

people, places, and situations. The grid formalizes this process and assigns mathematical values to the relationships between a person's constructs. Kelly grounded his theory in the mathematical relationships between the constructs. For example, he says (Kelly, G. A., 1959):

> "*Now let us turn to a personal system made up of a whole lot of constructs. Such a system is a complex, or, if you don't mind the term, a conceptual grid within which events can be seen in depth or in their psychological dimensions*".. p.13)

This formal approach has been applied in many different business management settings: to provide market research insights, improve quality controls, investigate motivation at work, facilitate negotiations, assemble teams, resolve conflicts, as well as other coaching/ counseling/ team-building applications (Stewart, Stewart, and Fonda, 1981).

Measurement Theory. A relational system is a set, together with one or more relations defined on the set. Measurement theory is the study of quantifying empirical relational systems through the construction of scales from the empirical relational system to a numerical relational system (Widmeyer, 1986). Abstraction is accomplished by the repertory grid technique, to represent real world situations (such as identity fraud potential) as a series of empirical relations (constructs). However, the repertory grid gives us only limited help with the measurement function, necessitating reference to measurement theory for further insights. With regard to the constructs, measurement theory will help to determine appropriate representation (normative, descriptive, axiomatic) and utility (uniqueness, consistency, additivity).

Index Number Theory. In economics, an index is a measure: a function F: D → R that maps a set of economically interesting objects D into the set R of real numbers, and that satisfies a system of economically relevant conditions (such as monotonicity, homogeneity, or symmetry conditions). The function values of the index F are index numbers. Perhaps the most frequently studied economic phenomenon is inflation -- it may be as old as money. In the old testament (Haggai 1,6) we read "You earn wages only to put them in a purse with holes in it." The first

monograph on inflation was written by the 15th century philosopher Oresme referenced in (Thorndike, 1929); and (Copernicus, 1517) wrote the earliest empirical study of the subject. However, this research is not about inflation, and not even about economics, but about the subject of identity fraud. The intention here is to map a set of attributes in identity document types (corresponding to D), into the set of real numbers R. Nevertheless, many of the same conditions of symmetry, homogeneity, identity and replication are relevant, and must be considered in the process of developing a model that gives a valid credibility metric for identity fraud.

Repertory Grid Technique

George Kelly regarded mathematics as "the purest form of construing" (Hinkle, 1970). He brought mathematics into his psychological theory by creating the repertory grid -- simply another way of stating his theory of personal constructs (Kelly, G. A., 1989). Kelly himself wrote:

> "*A construct is like a reference axis. A basic dimension of appraisal, often unverbalized, frequently unsymbolized, and occasionally unsignified in any manner except by the elemental processes it governs. Behaviorally it can be regarded as an open channel of movement, and the system of constructs provides each man with his own personal network of action pathways, serving both to limit his movements and to open up to him passages of freedom which otherwise would be psychologically nonexistent.*"
> (Kelly, G. A., 1965), p.293).

A number of corollaries have been defined with regard to personal construct psychology (Fransella, Bannister, and Bell, 2004). Constructs are bipolar as Kelly states in his Dichotomy Corollary, arguing that we make sense of our world by simultaneously noting likenesses and differences. Constructs have a range of convenience. The Range Corollary states that a construct (or a subsystem of constructs) always operates within a context, and that there is a finite number of elements to which it can be applied by a given person at a given time so for example we categorize automation as high-tech or low-tech, or numbers as integers or non-integers. However to consider automation as integer or non-integer makes no sense.

The Organization Corollary reads as follows: "each person characteristically evolves for his convenience in anticipating events, a construction system embracing ordinal relationships between constructs". Kelly suggests that construct systems are hierarchical with constructs standing to each other in what he terms subordinate and super-ordinate relationships. This is recognized in formal logic, in that mode of transport subsumes land based vehicles, which subsumes automobiles, which subsumes sport utility vehicles, which subsumes four-passenger sport utility vehicles, and so on. Early grid studies such as those of (Hinkle, 1965), with his description of "laddering", and (Landfield, 1971), with his description of "pyramiding", have focused on the organizational qualities of construct systems.

The Individuality Corollary states simply that people differ from each other in the way in which they construe events. No one has ever responded to a stimulus. Rather, they respond to what they perceive the stimulus to be.

The Commonality Corollary states that "to the extent that one person employs a construction of experience which is similar to that employed by another, these processes are psychologically similar to those of the other person." The Sociality Corollary states that "to the extent that one person construes the constructs and processes of a novel, he may play a role in a social process involving the other person". This is key because it describes how we try to understand others, and implies that to construe the constructions of another person is not simply to hold or mimic those constructions.

The Choice Corollary is the main motivational corollary of personal construct theory. It states that "a person chooses the pole of a construct that is likely to lead to the greater elaboration and extension of his or her system". This means we will choose that pole of a construct most likely to lead to or making increased sense of our world, though this choice may not be made at the conscious level.

Use of repertory grid interviews. Using personal construct systems in research is difficult because individuals normally do not have direct access to the structure of their own cognitions (Walsh, 1995) and usually know more than they can verbalize (Hufnagel and Conca, 1994). Understanding how people perceive the details of their work, and the similarities and differences among them, is critical to understanding the connections they make in evaluating new stimuli (Polanyi, 1966), such as the identity document types in this research. Nevertheless, the repertory grid method was used for conducting this research, for a number of reasons. First, it seemed to provide a very useful tool for engaged scholarship, in that it engages experienced professionals to articulate their experience to the researcher, rather than the researcher setting the boundaries for the interaction. Second, it is essentially a technique for conducting semi-structured interviews. Third, and most important, it provides a technique that effectively avoids researcher bias.

It is different from the more traditional interview methods that start with a fixed set of questions relating to the researcher's theoretical model. Such interviews tell participants what we want to know, and by exclusion, what we do not want to know. The researcher then leads the participants to provide particular explanations of the details selected by the researcher, stemming from the more general question. This has the disadvantage that the researcher will never gain knowledge from questions not asked. The repertory grid interviews by contrast, explore how the participants see their worlds. The researcher does not provide any theoretical framework that may bias the participants' answers. The repertory grid interview method reverses the interview process, starting with specific items of participants experience, and moving toward more general explanations (Davis, C. J. and Hufnagel, 2007), to try and understand the logic by which the participants differentiates or integrates these items of experience.

Identify the Elements - Types Of Identity Document. An important requirement for choosing elements is given by the Range Corollary. Elements should be within the range of

convenience of the constructs used. Kelly defines elements as "the things or events which are abstracted by a construct" and sees them as "one of the formal aspects of a construct." For example, the interviewer may ask the subject to think about the kinds of documents requested for evidence of identity, with respect to opening a new account, "What are the types of identity documents (elements) that you might ask for?"

Selecting participants. As described earlier, this research is focused on the financial services sector, and specifically on the opening of new accounts, the time when the organization typically has the highest exposure. Ten of the major financial service organizations in the South Florida area, banks and credit unions, were initially contacted. Eight of these organizations responded. Because the South Florida area has a relatively high percentage of international banks and customers with international backgrounds, it was fortunate that this provided a relatively high number of professionals with many years of experience in evaluating a variety of US-based and international identity document types. The eight responding organizations were requested to identify six to eight participants, those considered most experienced with the process of evaluating identity documents when opening new accounts; some provided as many as six individuals, one as few as two. These individuals were primarily in retail banking, but some also were involved with wealth management. A total of thirty-three individuals participated in the first round of interviews.

Identifying elements. Telephone conversations were conducted with one or two of the most experienced individuals at each responding organization, to identify the most frequently presented types of identity documents. This information was used to develop the following twelve elements used in the repertory grid interviews. Each element represents a specific type of identity document.

1. Costa Rica Birth Certificate (representative of any foreign birth certificate)
2. Business Card
3. Employee Identification
4. Florida Drivers License
5. “Green” Card
6. Jamaica Passport (representative of any foreign passport)
7. Master Card
8. Social Security Card
9. US Passport
10. Medical Insurance ID Card
11. Voter Registration
12. American Express Gold Card

Construct Elicitation - Components of Credibility. Kelly defines the Dichotomy Corollary of a construct as "a way in which two or more things are like and thereby different from a third or more things". For example, the interviewer may direct the subject to think about one triad of elements: Florida driver’s license (E1), a Visa credit card (E2), and an employee picture-identity (E3); then for each possible combination of three elements, ask for bipolar constructs that describe how two elements are alike, but different from the third. Answers could be:

- E1.E3 are alike because they have a clear color picture of the person, E2 is different because I don’t know if it belongs to the person.

- E1.E2 are alike because they come from well-known sources, E3 is different because the source may be unknown.

- E2.E3 are alike because they do not have a holographic image, E1 has a hologram, so it is hard to tamper with it.

Now we have three constructs --

1. picture included <---> no visual representation of holder

2. electronic medium <---> paper only

3. hologram included <---> no hologram; less tamper-proof

The first round of interviews, each lasting approximately one hour, was used to capture the sense-making information that these identity document experts use in their evaluation of the credibility of identity documents presented when new accounts were opened. The script used to introduce each interview is included as Appendix One. .

Three closing questions were asked to finish each first round interview. The first question was to find out which two of the list of identity document types were considered to have the highest credibility. The most frequently identified documents were the US passport and the Florida driver's license. The second question asked was which type of identity document was most different from all of the others and why. The most frequently identified document for this question was the business card, because it provided little personal information and was therefore not even considered to be a reliable type of identity document. The third question asked participants to identify any trends based on their experience, that have the potential to completely change the way they go about evaluating identity documents.

Laddering Up And Down - Getting the Details Right. As each interview was conducted, a technique called "going up the ladder" (Bannister, Mair, 1968) was applied to elicit details of why differences between elements were important to understand what makes the identity document type seem credible. Typically the process of "going up the ladder" to get to the real meaning of the construct is accomplished using why questions, to get to the most important aspect of the construct. A simple example of the sequence of questions and answers might be as follows.

Q. Regarding the picture, why is it important to you?

A. I can tell right away if the right person has the ID...

Q. Why does that make a difference to you?

A. Well, there is a better chance the ID is good, if the picture matches the person.

Q. And why is that? etc.

The process of "laddering down" (or "going down the ladder" or "pyramiding") was used to get more details of a construct described too broadly by the participant. "Going down the ladder" is accomplished using how questions to get to any multiple characteristics that may exist in the original construct elicited. The question-and-answer sequence might look like the following.

Q. Regarding the source of the ID document, tell me more about how a well-known source is different?

A. It means they are more experienced making documents not easily falsified.

Q. Can you give me some more examples of how a well-known source is different?

A. Maybe they have been in existence longer, or they are part of the federal government.

Q. How does this make them different? etc.

Full Grid - Assigning a Scale. Ask the interviewee to rate each element (the identity document type) on a construct scale, usually a 5-point scale. For example:

Q. With regard to visual representation, scale of 1=poor, to 5=best, how does employee-ID rate?

A. As a 4 --better than a visa card, but not as good as a Florida driver's license.

Q. For the electronic medium, on a 1-5 scale how would you rate the visa card? etc.

This would have the positive effect of improving the measurement of the component from a categorical to an ordinal measurement. This final stage of the repertory grid methodology, the full grid, has been postponed for future research for a number of practical reasons.

1. The primary objective of the research was to identify the different characteristics that seem to make identity document types credible. This was accomplished effectively by the first round of interviews. The completeness of the list of characteristics was validated in two ways. During the first interview, each participant was asked if any document types appeared to be missing from the list, to make certain that all types (and their associated characteristics) were considered. During the second interview, each participant was asked if there were any attributes missing from the list of twenty-one, attributes that they think about when evaluating credibility for opening a new account.

2. The secondary objective of the research was to develop a composite rating of the different characteristics of credibility, a rating that can be used for any documents, rather than to compare the credibility of the twelve specific documents used as elements in the repertory grid.

So an alternative approach was taken in the second round of interviews to develop a rating of the importance of each characteristic. As described above, each participant, for each scenario, rated each characteristic on a scale of 1 to 5. General validation of the approach is provided by the fact that the two highest rated document types indeed have the highest rated characteristics, while the lowest rated document type has the lowest rated characteristics. Further development of a credibility index is limited by the small sample of participants, and by the need for a more rigorous validation, so that the objective remains for further research.

Hypothetical Scenarios

Defining Scenarios. Scenarios have been defined as "…tools for ordering one's perceptions about alternative future environments in which one's decisions might be played out." Alternatively: "…a set of organized ways for use to dream effectively about our own future" (Schwartz, 1991). Scenarios usually include plausible, but unexpectedly important situations and

problems that exist in some small form in the present day. Any particular scenario is unlikely. However, analysts in future studies may select scenario features so they are both possible and uncomfortable. Scenario planning helps policy-makers to anticipate hidden weaknesses and inflexibilities in organizations and methods (wikipedia.org, 2007b).

Another term that is commonly used is "vignettes," which typically refers to short "storylines" illustrating one or other facet of a scenario – one person's daily experience, for instance. Fine-detail concepts may be used for organizational arrangements, sub-cultural practices, management philosophies, and so on. A vignette is typically made up of such fine details, and situated within a wider scenario (Miles, Green, and Popper, 2004). The concept of the vignette is more appropriate for this credibility research, with its fine focus on identity document credibility, rather than a broader focus on general business strategy. However, the terms scenario and scenario-planning will be used throughout, to maintain consistency with the general literature.

We can use scenarios to define and understand the impact of external forces and triggers that may affect the future; to envision what new crises may erupt; and to evaluate and refine policies and plans developed using other methods (Heyer, 2004). The effectiveness of scenario planning depends on facilitator's ability to engage organizational members in genuine conversation about the possibilities of the future. The scenario planning process is one of dialogue, challenge, and willingness to re-examine ideas. Thus, participants must be comfortable engaging in conversation and must be open to having their ideas challenged by other participants. By definition, learning happens when people begin to see new things or existing things in a new way (Chermack, van der Merwe, and Lynham, 2007). A critical success factor in the scenario planning method is that there is a real interface of the scenarios with the managers. Merely quantifying the outcomes of obvious uncertainties is not enough. Managers must create a new

mental model of the business environment -- meaning that the scenarios cause the managers to "re-perceive reality" (Wack, 1985). For example, some of these re-perceptions in the world of identity documents could be: (1) the emergence of digital customers, where the organization never meets a physical person, or (2) identity evidence flow networks, where there are no physical identity documents, or (3) a single identity document represents multiple relationships with issuing organizations.

Mental Models

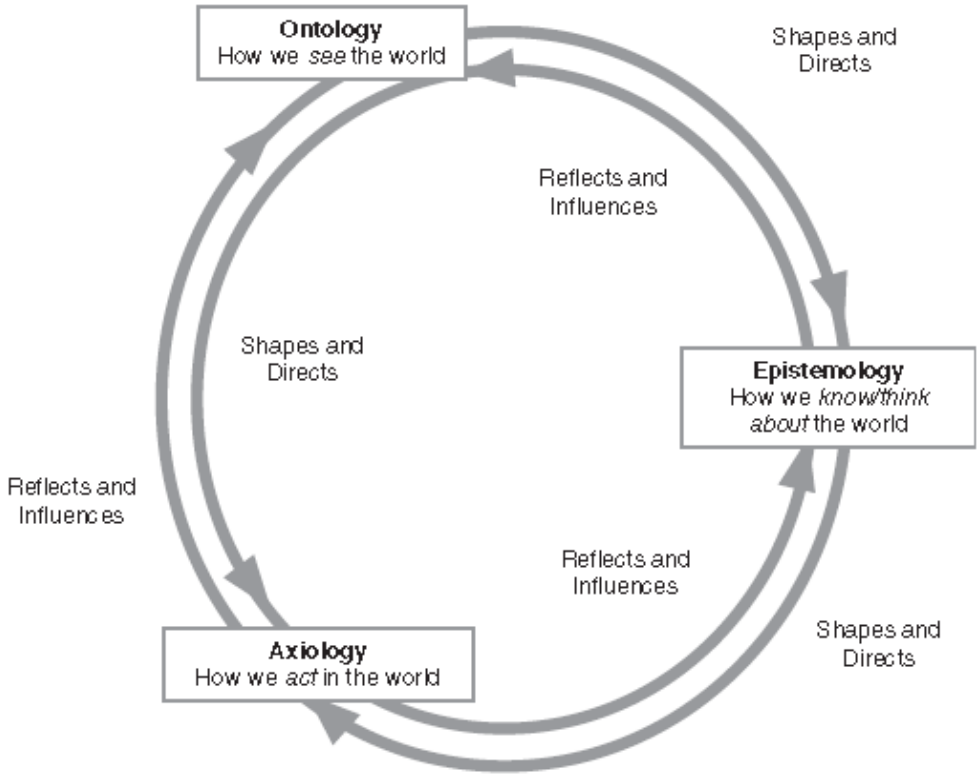

Figure 5. Ruona And Lynham's System of Interacting Components of Thought and Practice

A good illustration of how managers mental models affect their actions (Figure 6) comes from Ruona and Lynham's System of Interacting Components of Thought and Practice (Ruona and Lynham, 2004). It is useful for illustrating the relationships among mental models and

human perceiving, thinking and acting. Mental models include the biases, beliefs, experiences, and values of individuals (Ford, D. N. and Sterman, 1998) and are constantly interacting with patterns of perception, thought and action. Scenarios attempt to change the epistemology.

Scenarios have been examined in decision theoretic terms (Bell, 1982); from an economic perspective (Porter, 1985); in business planning terms (Raubitschek, 1988); and from a forecasting angle (Huss, 1988). The Repertory Grid technique has been shown to complement the scenario methodology, by allowing analysts to elicit requirements in scenarios where they do not have specific "business knowledge" (Davis, C. J., Fuller, Tremblay, and Berndt, 2006).

Scenario Construction: Four Scenarios. The following ten steps in scenario construction are well described in the literature, for example, (Schoemaker, 1993), and so will be used as the guide for this research.

1. Define the issues you wish to understand better (for example, credibility attributes in identity documents as they change during the next five years).
2. Identify the major stakeholders or actors who would have an interest in these issues, both those who may be affected by it and those who could influence matters appreciably. Identify their current roles, interests, and power positions.
3. Make a list of current trends or predetermined elements that will affect the variable(s) of interest. Briefly explain each, including how and why it exerts an influence. Constructing a diagram may be helpful to show inter-linkages and causal relationships.
4. Identify key uncertainties whose resolution will significantly affect the variables of interest to you. Briefly explain why these uncertain events matter, as well as how they interrelate.
5. Construct two forced scenarios by placing all positive outcomes of key uncertainties in one scenario and all negative outcomes in the other. Add selected trends and predetermined elements to these extreme scenarios.

6. Assess the internal consistency and plausibility of these artificial scenarios. Identify where and why these forced scenarios may be internally inconsistent (in terms of trends and outcome combinations).
7. Eliminate combinations that are not credible or not possible, and create new scenarios (two or more) until you have achieved internal consistency. Make sure these new scenarios bracket a wide range of outcomes.
8. Assess the revised scenarios in terms of how the key stakeholders would behave in them. Where appropriate, identify topics for further study that would provide stronger support for your scenarios, or might lead to revisions of these learning scenarios.
9. Examine the internal consistencies of the learning scenarios and assess whether certain interactions should be formalized via a quantitative model.
10. Reassess the ranges of uncertainty of the dependent (i.e., target) variables of interest, and retrace Steps 1-9 to arrive at decision scenarios that might be given to others to enhance their decision-making under uncertainty.

The six trends identified from the interviews are described below, in two groups.

High Tech:

1. Increasing use of advanced biometric data as part of the identity document.
2. Increasing use of electronic media as part of the identity document.
3. Increasing emergence of virtual customers – – physical presence not required to open new accounts.

Strong Authentication Procedures:

4. Emergence of a single centralized agency with the authority to issue the only legal identity document.

5. Increasing requirement for ID-document issuing agencies to validate identity information, and to create a tamper-proof document at the time the ID is issued.
6. Increasing requirements for real-time access to an online authentication database.

Using the ten-step method, four scenarios were created by grouping the six trends into two sets of three as shown in the two-by-two matrix below. Scenario #1 was contrived to be the closest to a current situation, and #4 as the most futuristic, without being unrealistic.

Six trends (2 groups of 3) Four Scenarios	**Weak authentication** 4. Decentralized ID-Process 5. Picture-signature-text plastic.card 6. Offline authentication	**Strong authentication** 4. Single, central ID Issue 5. Validated, tamperproof ID 6. Real-time authentication
Low-tech. 1. Simple or no biometrics 2. Simple or no electronics 3. Customers' physical presence required	**1** (current)	**3**
High-tech. 1. Advanced biometrics 2. Advanced electronics (RFID) 3. Virtual customers (and digital ID)	**2**	**4** (future)

Figure 6. Trends and Scenarios for Identity Document Evaluation

Evaluating Results

The relative importance of each of the characteristics of credibility was determined by evaluating the constructs derived during the first round of interviews, under each of the scenarios created. This process was accomplished by a second round of interviews with 40 experts, including the 33 interviewed during the first round. A predetermined script was used to describe

the requirements to the interview participants, to ensure that no bias was introduced by the process. This script is included as Appendix Two. .

VIII. SUMMARY AND DISCUSSION OF RESULTS

As described in the background section, this research is significant for three reasons. First, the repertory grid interviews elicited the attributes of credible identity document types, in response to the first part of the research claim that measurement of identity document credibility is a good metric for potential identity fraud. The elicited attributes give new insight to understanding the nature of the indicators that should be the focus in developing identity document standards, and developing solutions for the identity fraud problem. These conclusions are further supported by the fact that the elicited attributes represent the use of RGI as an inter-organizational knowledge acquisition tool, to create a pool of expert knowledge, acquired individually, and then combined across all organizations for evaluation of the importance of each attribute.

Second, the research represents an application of engaged scholarship. Rather than simply reviewing the results of other related research, the experts were interviewed individually, and asked to define the credibility attributes and their values in different scenarios. The experts suggested that these values could be applied as a metric for potential identity fraud, a positive response to the second part of the research claim. Further research is needed to confirm these values, and eliminate any overlaps among the attributes. However, the existence of the metric gives organizations a tool that could be used to determine the best types of document to be used for identity validation, and to estimate the identity fraud risk associated with new types of identity documents that may emerge.

Third, the increasing number of entities that both create identity documents, and review documents created by other entities, comprise a complex inter-organizational network. Ongoing growth of this network of identity token flows is increasing the value and corresponding risk of fraudulent access to organizational information and assets, and is therefore increasing the need for creative new methods of fighting the identity fraud problem. This research suggests a potential new weapon to carry on this fight, by continuing to develop standards and requirements for identity document issuers, and by setting appropriate organizational policies to require identity document types, or combinations of types.

Contributions to Literature: Identity Theft, Personal Construct Theory, Credibility

This research was designed to answer two critical questions about credibility in identity documents. The first question is, "What attributes do individual experts perceive that make identity documents credible?" Describing the attributes of credible identity documents allows for better understanding of the indicators of potential identity fraud. That should be the focus in developing solutions for the identity fraud problem. The second question is, "How does the expert group rate the importance, for predicting fraud potential, of each item on the aggregate list of perceived attributes?" Measuring identity fraud potential can provide a tool for selecting the most useful identity documents.

Intuitively, it may seem that there should be an analytical answer to the first question of what are the most important attributes of credibility. However, this is not the case, and so research like this continues, in order to develop non-analytical answers to the question. Any presently conceivable attribute can be compromised, and as quickly as technology changes to thwart criminals, the criminals change methods to beat the technology. For example, fingerprint verification is often considered a highly secure means of validating identity. However, in 2000, a

Japanese researcher showed how easily a fingerprint could be forged with a gelatin strip. Evidence of this forgery was then removed quickly and discreetly simply by sucking the finger. Biometric data is also considered a secure means of validating identity. However, electronic records of biometric data can be copied and included in a fraudulent document. Sometimes, the security comes from some special physical media used for certain identity document types. Passports are created in special booklets with secure paper. However, these can also be subjected to fraud (Dateline-NBC, 2007). US border inspectors have a hard time detecting passports known as stolen blanks, i.e., real documents taken from official stock before they have been filled out. Illicit brokers steal them, or buy them from corrupt officials. Moreover, according to the dateline report:

> "*Of all the types of fraudulent passports, what concerns authorities the most is a genuine passport issued by a government agency under a false identity. The British government unwittingly issued two passports to al-Qaida operative Dhiren Barot under two different false names.*"

Identity Theft Literature. A literature review was conducted to help develop a research basis to answer the questions about the most important attributes of credibility. As this effort proceeded, it became clear that a number of different literature streams would need to be reviewed. The first area reviewed was literature related to identity theft. In general, the discovery here is that responses to the problem of identity theft are being developed along a number of fronts. Law enforcement is responding, various legislative bodies are responding, researchers are responding, industries are responding, and the victim groups are responding. In general, the literature review showed steady increase is in the size of the identity fraud problem, especially from the year 2003 through the year 2006. Then, a decrease first appears in year 2007. However, one constant throughout is the fact that the new account fraud continues to be the most costly and difficult to repair. One interesting fact has emerged from the literature review in this area. It gave us the methodology for calculating credit scores. An individual credit score is based

on an analysis of risk factors associated with the individual and the situation. This research has added to the identity theft literature, as it presents a methodology that provides an objective analysis of experts perceptions of the risk factors associated with identity document credibility. After all, human experts usually make the final decision about accepting or rejecting an identity document.

Credibility Literature. Another stream of literature needed to be reviewed to understand the constructs that underlie the concept of credibility. Some of these constructs include persuasiveness (as in credible speakers), source-message-media (as in credible journalism), trust and belief (as in credible Internet sites), information quality (as in credible journal articles), cognitive authority (as in credible professors, doctors, or librarians), and expertise (as in credible expert systems).

However, all the researchers agree that there are limitations to these lines of research. Often, the constructs are not generalizable across different contexts. In particular, in the context of identity documents, it is important to understand the perceptions of the individuals making decisions about their acceptance. Is the document an explanation of holder privileges, a claim to assets provided by the organization, or simply a verification of some inherent holder characteristic? Organization and situational contexts may also lead to over or under reliance on these constructs. Another serious limitation is the presence of subjective factors. A researcher may use terminology that is foreign to the participant, or it may be difficult to distinguish whether identified attributes are predictors of document credibility, or really an underlying dimension of the construct.

This research contributes to the credibility literature, by adding a new set of constructs unique to the context of identity document credibility, constructs that relate to identity documents and their potential for identity fraud. This approach overcomes most of the limitations described

in the previous paragraph. The results are not general, but specific to the context of identity documents. The individual experts have the same perceptions of the situation, as the setting defined is that of opening a new account; all of them are implicitly or explicitly aware of the risks of new account fraud. The repertory grid methodology provides an objective approach, free of researcher bias, as the experts define the constructs in their own terms.

Personal Construct Literature. From reviewing the credibility literature, it seemed clear that a rigorous basis was needed to support the idea of constructs as they relate to the abstract concept of credibility, and so the second stream of literature reviewed was related to George Kelly's theories on personal construct psychology. The details have been discussed elsewhere in this document, but are summarized here to show where the literature ends, and the contribution of this research begins. Personal construct psychology tells us that people construct reality by creating constructs, as ways of viewing their world. These constructs apply to "anything we pay attention to". Then with experience, and the development of expertise, we refine our theories to make our world more predictable. The repertory grid is a practical application of personal construct psychology, where a therapist helps a subject define her own constructs, instead of imposing his own. Repertory grid interviews (RGI) are a specific format for semi-structured interviews, originally developed to help a therapist explore someone's construct system and understand how they see their world. It does not start with questions fixed by the therapist/researcher, but rather allows free-flowing discussion, where participants describe their own thinking in their own words.

This research has added to the personal construct literature, with another application of repertory grid interviews as a knowledge acquisition tool. RGI is a repeatable process for the pooling of inter-organizational expertise and experience. The researcher interviews individual experts in their world of reviewing and identity documents for credibility, to elicit their

constructs, the attributes of identity documents that they perceive in evaluating the likelihood that the document is not fraudulent. These individual expert interviews are compiled to produce a composite list of these credibility attributes, and then the experts asked to rate the importance of these attributes in different scenarios.

Contributions to Theory and Practice - Characteristics of Credibility

A qualitatively rich data set was gathered during the first round of interviews. All participating organizations allowed recording of the interviews, except one (four participants), for a total of 29 recordings in 33 interviews. The amount of participant experience in reviewing identity documents ranged from 10 to 35 years. There were 22 females and 11 males. During this first round of interviews, there were a number of interesting, and sometimes surprising, participant (P)/ researcher (R) conversations, not directly related to the repertory grid data. Some examples are:

R: "For instance, one of the numbers on your Florida driver's license tells you if you are male or female ..."
P: "I am realizing that I need to focus more consciously on these documents when I'm looking at them. There are so many little things that are easy to miss."
- - -
P: "your comment about new account fraud makes me worry much more about credible identity documents."
- - -
R: "... thank you for taking the time to do this ..."
P: "This was a very useful hour for me. Now when I'm opening a new account I will think about what I think about. Does that make sense?"

The primary focus of this research is to explore what indicators of fraud potential exist on different types of identity documents, and to develop metrics that answer the question, "What attributes make identity documents seem credible?" The results of the first round of interviews represents a major contribution to the theory related to identity fraud research, as it provides a

qualitative answer to the question, based on knowledge acquired from experts in a variety of organizations. The list identifies the specific indicators that experts focus on when opening a new account, to avoid being deceived by fraudulent documents. In addition, there is a substantial contribution to the practice of identity fraud mitigation, as the comments suggest strongly that the participants felt that the interview process was helpful in making them think about how they evaluate the credibility of the identity documents they review when a new account is opened.

The twenty-one characteristics of credibility are listed, i.e., the attributes of identity documents that make them seem credible for banking experts reviewing them as part of the new account opening process. Most are self-explanatory; the few exceptions include some brief discussion

1. Authentication database. This is an external characteristic, where a database of identity documents from the outside exists to authenticate the data on an ID document presented.
2. Biometrics-advanced (DNA information, retinal scans, fingerprints)
3. Biometrics-simple (picture, signature, height, weight, eye color)
4. Coded-ID-Number. All identity documents have a unique numbers, but some numbers contain coded information. For example the first three digits of the Social Security number indicate the state where the number was issued. Similarly, the Florida drivers' license number includes information about gender, day of the month the holder was born, and so on.
5. Country-of-origin. Where the document holder was born.
6. Date-issued
7. Date-of-birth
8. Date-of-expiry
9. Document-electronics (barcode, magnetic stripe, RFID chip)
10. Document-medium (Digital-Plastic-Paper-Book)
11. Document-size
12. Employment-status/data
13. Full-Name
14. Gender
15. Government-issued (federal, state, local, foreign, other)
16. Home-address
17. Issuer-reliability (validated-data, etc.)
18. Photo
19. Risk-to-security low ratio. A high ratio means: there is a <u>high</u> risk exposure associated with successfully presenting a fraudulent identity document, while at the same time, security features on the document are at a relatively <u>low</u> level, resulting in a high risk to security ratio.
20. Signature
21. Tamper-proofing (laminates, seals, holograms)

In addition to identifying the indicators of potential identity fraud, note the importance of this list as a pool of inter-organizational expert knowledge, acquired through this research. This represents an important addition to theory, both as an inter-organizational method of expert knowledge acquisition, and as a list of characteristics for identity documents to be considered less susceptible to identity fraud. Recall that another area of research interest is to determine if these characteristics of credibility can be used as metrics for potential identity fraud. One example of a conversation during the first round of interviews is typical of others that suggested that credibility in identity documents is not distinguishable from potential for fraud, i.e., that credibility is in fact a measure of that potential:

P: "This is a very useful process. I'm usually so busy that I don't have time to think about how I make my judgments about fraudulent documents.
R: "Is a credible document the opposite of a potentially fraudulent document?"
P: "Well, yes. I guess so. If I think the document is credible -- if I believe what I'm seeing -- then it means I don't think it's fraudulent, right?"
R: "That's my question to you."
P: "Oh, right! Yes, if a document is credible, that means it's not forged."

The second round of interviews included 43 participants, as the 10-year minimum experience requirement was relaxed. Experience in this round ranged from 4 to 35 years. There were 30 females and 13 males. It is worth noting, that when the composite list was presented to each of the experts at the start of their second round interview, there was an almost 100% reaction of very strong interest, as they recognized characteristics that they had not previously identified. This represents another significant contribution to practice, suggesting that this inter-organizational pooling of knowledge would be very useful to all financial service organizations.

Many studies show that credibility does not reside in the information object or source itself. Rather, the users recognize dimensions of credibility based on the characteristics of information objects and sources and then make credibility judgments. In other words, although objects and sources provide clues that can be used to make information more believable,

individuals will eventually make different assessments of information because of their experiences and knowledge. In relation to this research, the experts interviewed would be expected to identify similar characteristics of the identity documents, but their evaluation of these characteristics as metrics of potential identity fraud, would differ according to their experience. Also, credibility perceptions may change over time, (Metzger, Flanagin, and Zwarun, 2003). For example, the credibility of online political information in the USA changed from the 1996 to the 2000 election season, (Johnson and Kaye, 1998, 2000, 2002).

In this research, the experts' judgment would be expected to change with time and environment. This situation was simulated by using four different scenarios as described in Chapter 6. The six trends identified during the first round of interviews are repeated here for convenience:

1. Increasing use of advanced biometric data as part of the identity document.
2. Increasing use of electronic media as part of the identity document.
3. Increasing emergence of virtual customers - physical presence not required to open new accounts.
4. Emergence of a single centralized agency with the authority to issue the only legal identity document.
5. Increasing requirement for ID-document issuing agencies to validate identity information, and to create a tamper-proof document at the time the ID is issued.
6. Increasing requirements for real-time access to an online authentication database.

This represents another contribution to the practice of identity fraud mitigation, as the experts define the trends in the financial service industry, and describe how these trends could affect their evaluations of the importance of attributes present on identity documents.

In the sections that follow, the repertory grid "focus" graphic for each scenario is included, together with some brief analysis of the information conveyed. Some discussion is warranted to understand the focus graphic. Each labeled row in the graphic represents one of the twenty-one characteristics on the composite list developed from the experts who participated in the first round of interviews. Each column in the graphic represents the evaluations from one of the experts who participated in the second round of interviews. Column labels are excluded to preserve anonymity of the participants. The rows are sorted so that those most similar to each other in values appear closest to each other towards the center. The tree structure to the right of the columns shows the measure of similarity.

So for example in Figure 8, importance of "photograph", and unimportance of "advanced-biometric" are a sub-cluster with about 95% similarity (less than 5% difference) in rating among all 38 second-round participants, and each of these are just under 95% similar to the rating of importance of the "signature" attribute.. In the same figure, the importance of another sub-cluster, "date-of-birth" and "date-of-expiry", are rated about 95% similar (only 5% difference among all round two participants. The sub-cluster [photograph + advanced-biometric + signature] is slightly more than 90% similar to the sub-cluster [date-of-birth + expiry-date]. Finally, we can see from the graphic that the cluster of these five constructs are no more than 10% different from each other in terms of the expert ratings of importance in this scenario.

Scenario 1 Description and Analysis. In scenario number one, the identity document:

- Could be issued by any third party – government, employer, insurance company, etc.
- Data includes a photo and signature.
- Is plastic or laminated, and about the size of a credit card
- Data can be authenticated, but offline; needs about 24-48 hours.

- Has little or no biometrics, little or no electronics.

- The customer must be physically present when opening the new account.

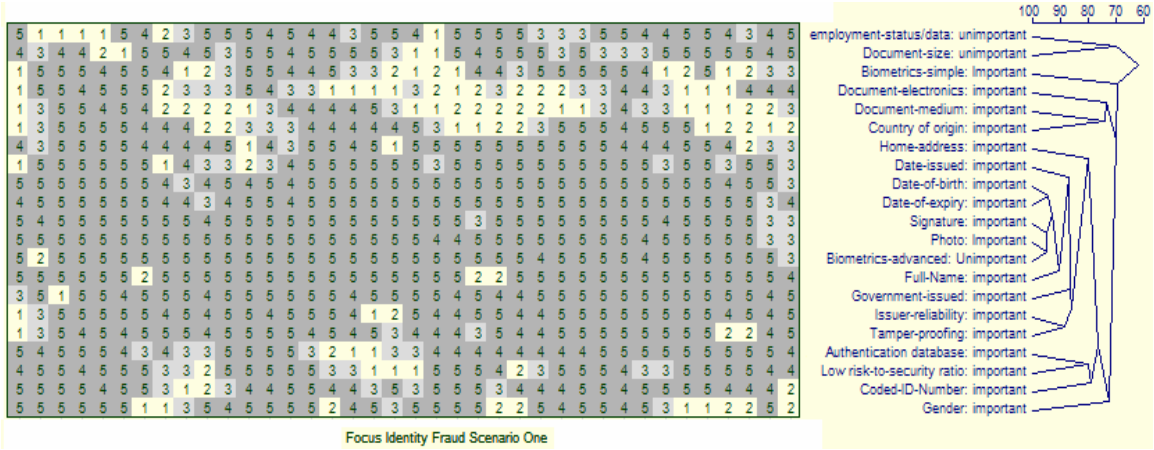

Figure 7. Repertory Grid Focus Scenario One

Avg.	Std.Dev	Construct
4.8	0.5	Date-of-birth: important
4.8	0.5	Photo: important
4.8	0.6	Signature: important
4.7	0.5	Date-of-expiry: important
4.7	0.8	Full-Name: important
4.7	0.8	Government-issued: important
4.4	1.0	Issuer-reliability: important
4.3	1.2	Date-issued: important
4.3	1.0	Tamper-proofing: important
4.2	1.0	Coded-ID-Number: important
4.2	1.1	Home-address: important
4.1	1.1	Authentication database: important
4.0	1.3	Low risk-to-security ratio: important
3.8	1.5	Gender: important
3.5	1.5	Biometrics-simple: important
3.4	1.4	Country of origin: important
2.9	1.4	Document-electronics: important
2.6	1.3	Document-medium: important
2.2	1.4	employment-status/data: unimportant
1.9	1.2	Document-size: unimportant
1.2	0.6	Biometrics-advanced: unimportant

Table 1. Construct Importance Ratings Scenario One

The most similar, highest-ranked characteristics in scenario one are photograph, signature, date-of-birth, and date-of-expiry. This confirms intuitive expectations, given the context described for scenario one. Both the document and the new customer are physically present. The high-ranked items can all be visually confirmed. The lowest ranked characteristic (a mirror image of the photograph attribute) is biometrics-advanced. This also confirms intuitive expectations, as scenario one explicitly describes the situation where little or no biometric data are present on the identity document. However, what is quite unexpected in this scenario is that issuer-reliability and tamper-proofing are similarly rated (about 85%), but relatively low in order, falling to the middle of the list.

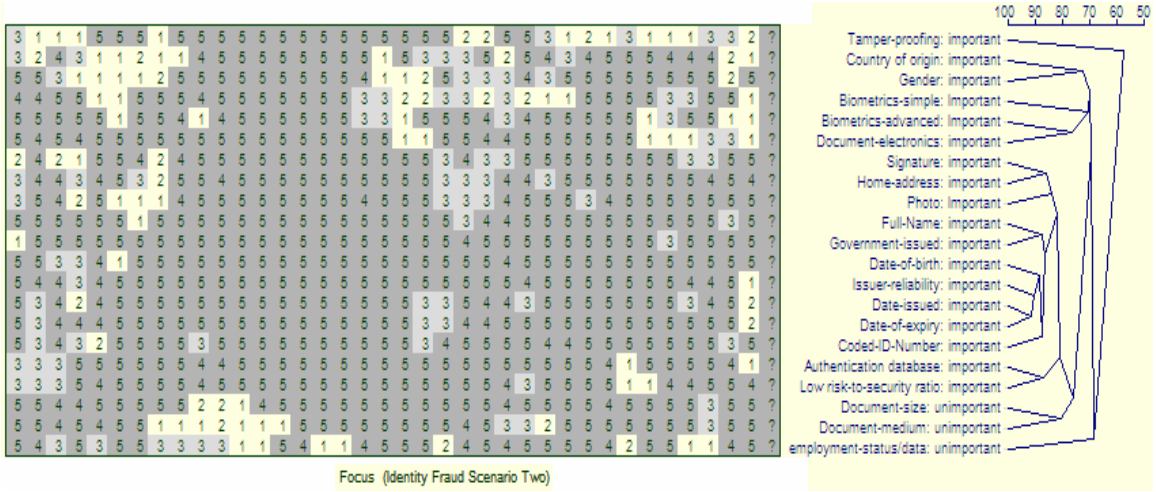

Figure 8. Repertory Grid Focus Scenario Two

Scenario 2 Description and Analysis. In scenario number two, the identity document:

- Could be issued by any third party – government, employer, insurance company, etc.
- Data includes a photo and signature.
- Is plastic or laminated, and about the size of a credit card
- Data can be authenticated, but offline; needs about 24-48 hours.
- Contains advanced biometrics (for example, DNA, retinal scans, fingerprints)

- Contains advanced electronics (RFID chip contains electronic form of all data, and it is continuously transmitting, so that the identity document can be tracked at all times)
- Is digital, not physical
- The customer is virtual, need not be physically present when opening the new account.

Figure 9 shows the most similarly ranked characteristics are date issued, date of expiry, issuer-reliability and date-of-birth. In comparison to scenario one, note that photograph and signature are now rated differently, perhaps because this scenario stipulates that the customer is virtual not physically present and the identity document is digital, also not physically present.

Avg.	Std.Dev	Construct
4.8	0.7	Government-issued
4.7	0.8	Date-of-birth
4.7	0.8	Full-Name
4.7	0.8	Issuer-reliability
4.6	0.7	Date-of-expiry
4.5	1.0	Authentication database
4.5	0.8	Coded-ID-Number
4.4	0.9	Date-issued
4.4	1.1	Low risk-to-security ratio
4.3	0.9	Home-address
4.3	1.1	Signature
4.2	1.2	Photo
4.1	1.5	Document-electronics
4.0	1.5	Biometrics-advanced
3.8	1.6	Gender
3.7	1.5	Biometrics-simple
3.5	1.5	Country of origin
3.4	1.7	Tamper-proofing
2.3	1.5	employment-status/data
2.1	1.5	Document-medium
1.5	1.0	Document-size

Table 2. Construct Importance Ratings Scenario Two

The highest rated characteristics in this scenario are government-issued, issuer-reliability, date-of-birth, full-name, and date-of-expiry. We may speculate that government issued, and

issuer-reliability are different ways of saying that the experts now rely on the reputation that the document issuer has for creating documents that have reliable data with a low potential for identity fraud. The lowest rated attribute is document size – a logical result since the document not being physically present means the size cannot be seen.

Scenario 3 Description and Analysis. In scenario three, the identity document:

- Is legally issued only by a single centralized agency that could be either a government or a private organization.
- Is issued by a process that can be trusted to ensure that the data accurately represents the applicant at the time of issue, and that the document is tamperproof.
- Data can be authenticated on a real-time basis when the document is presented.
- Has little or no biometrics, little or no electronics.
- The customer must be physically present when opening the new account.

The *highest* rated characteristics in this scenario are Date-of-birth, Full-Name, Signature, and Date-of-expiry. Again, this is not surprising, given the visual presence of both new customer and the identity document under review. The *most similarly* rated characteristics are date-issued, date of expiry, signature and photograph. This disconnect between highest rated, and most similarly rated characteristics, is somewhat of a surprise. The lowest rated characteristics are Document-size, employment-status/data, and Biometrics-advanced. This low rating for employment-data is surprising, probably because identity-checking is primarily associated with credit capacity in the banking industry.

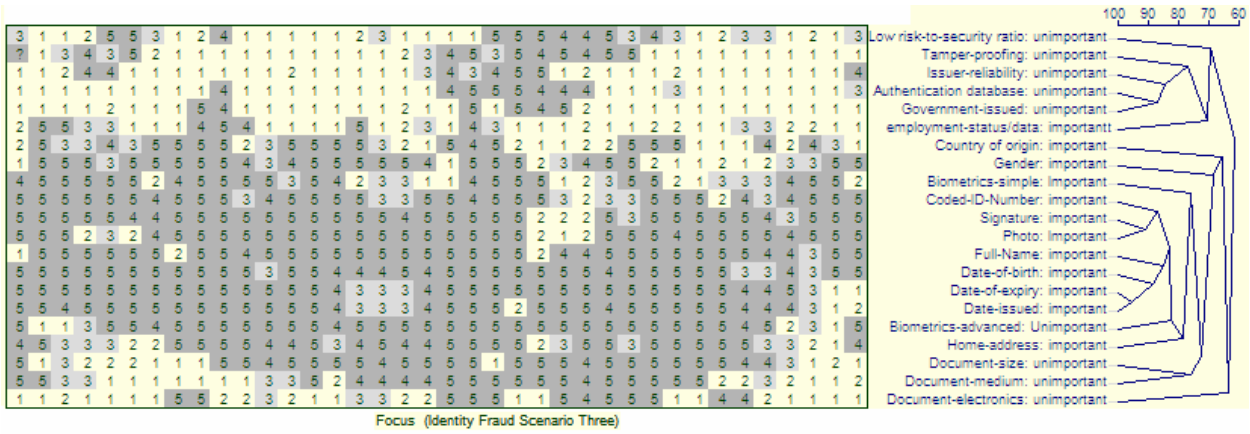

Figure 9. Repertory Grid Focus Scenario Three

Avg.	Std.Dev	Construct
4.6	0.7	Date-of-birth
4.6	1.0	Full-Name
4.6	0.9	Signature
4.5	1.0	Date-of-expiry
4.4	1.1	Photo
4.3	1.0	Coded-ID-Number
4.3	1.0	Date-issued
4.3	1.3	Government-issued
4.2	1.3	Issuer-reliability
4.1	1.4	Authentication database
4.0	1.2	Home-address
3.8	1.5	Gender
3.8	1.6	Tamper-proofing
3.7	1.4	Biometrics-simple
3.5	1.6	Document-electronics
3.5	1.5	Low risk-to-security ratio
3.3	1.6	Country of origin
2.7	1.6	Document-medium
2.3	1.6	Document-size
2.2	1.4	employment-status/data
1.6	1.2	Biometrics-advanced

Table 3. Construct Importance Ratings Scenario Three

Scenario 4 Description and Analysis. In the fourth scenario, the identity document:

- Is legally issued only by a single centralized agency that could be either a government or private organization.

- Is issued by a process that can be trusted to ensure that the data accurately represents the applicant at the time of issue, and that the document is tamperproof.
- Data can be authenticated on a real-time basis when the document is presented.
- Contains advanced biometrics (for example, DNA, retinal scans, fingerprints)
- Contains advanced electronics (RFID chip contains electronic form of all data, and it is continuously transmitting, so that the identity document can be tracked at all times)
- Is digital, not physical
- The customer is virtual; need not be physically present when opening the new account.

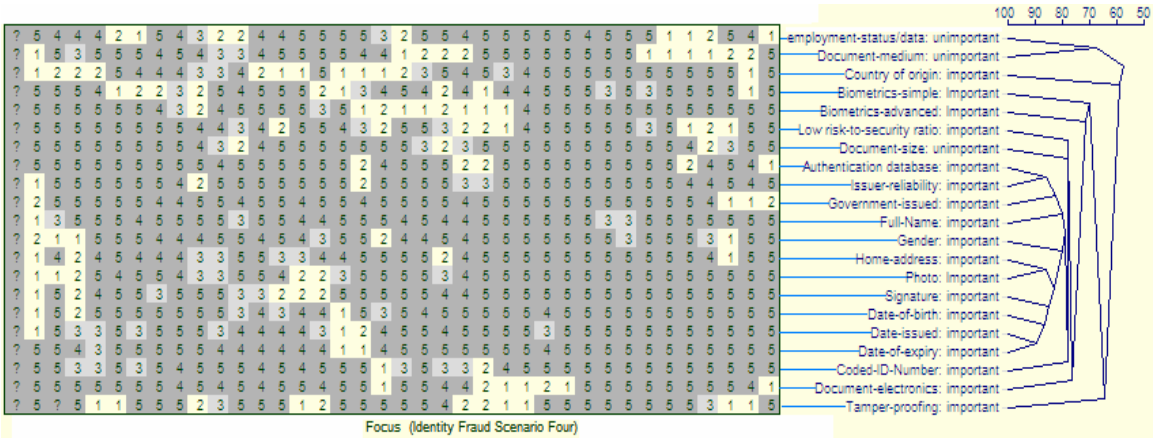

Figure 10. Repertory Grid Focus Scenario Four

The highest rated characteristics are authentication-database, date-of-expiry, full-name, and issuer-reliability. Not surprisingly, in a scenario where new customer and identity document are digital, AND the document issuing process is reliable and tightly controlled, experts tend to weigh heavily on the authentication database kept by the issuing agency. Most similarly rated characteristics are the three dates: date-of-expiry, date-of-birth, and date-issued. The lowest rated characteristics are document-medium, employment-status/data, and Document-size. Once more, this is not surprising given the absence of a physical customer and document. In summary, expert

evaluations of the identity document characteristics in different scenarios suggest that visual characteristics are most important for document types in their physical form, while authenticated personal data are most important for a document types in their digital form. Most surprising is that the characteristic of tamper-proofing falls so low in importance in all four scenarios.

Avg.	Std.Dev	Construct
4.5	1.1	Authentication database
4.5	1.0	Date-of-expiry
4.5	0.9	Full-Name
4.5	1.0	Issuer-reliability
4.4	1.0	Coded-ID-Number
4.4	1.1	Date-of-birth
4.4	1.1	Government-issued
4.3	1.2	Signature
4.2	1.1	Date-issued
4.2	1.2	Home-address
4.2	1.2	Photo
4.1	1.4	Document-electronics
4.1	1.3	Gender
3.9	1.6	Biometrics-advanced
3.9	1.4	Low risk-to-security ratio
3.8	1.4	Biometrics-simple
3.8	1.7	Tamper-proofing
3.5	1.6	Country of origin
2.4	1.6	Document-medium
2.2	1.4	employment-status/data
1.5	1.0	Document-size

Table 4. Construct Importance Ratings Scenario Four

Synthesis of results. The Table 5 synthesis shows the highest consensus across all scenarios (highlighted totals), on the dates: date-issued, date-of-expiry, and date-of-birth, all data related items. The highest rated overall included date-of-birth, full-name and signature, all visual items. There were surprisingly low ratings overall for biometrics, tamper-proofing, and employment data., which would have been expected to be high on the list of items for a bank, that

normally is interested in credit capacity. Meanwhile, on the contrary in Scenario 1, experts seem to agree on the low ratings.

The synthesized results suggest that the expert judgment, with their apparent preference for visual characteristics, may be somewhat out of sync with the banks and regulators. Based on anecdotal evidence, review of security related procedures, and on the author's experience with financial institution audits, the institutions and regulators seem to favor tamper-proofing, security, and other high-technology features, for identity theft protection.

	Construct	S1	S2	S3	S4	Total
7	Date-of-birth	4.8	4.7	4.6	4.4	18.5
13	Full-Name	4.7	4.7	4.6	4.5	18.5
8	Date-of-expiry	4.7	4.6	4.5	4.5	18.3
15	Government-issued	4.7	4.8	4.3	4.4	18.2
20	Signature	4.8	4.3	4.6	4.3	18.0
17	Issuer-reliability	4.4	4.7	4.2	4.5	17.8
18	Photo	4.8	4.2	4.4	4.2	17.6
4	Coded-ID-Number	4.2	4.5	4.3	4.4	17.4
3	Authentication	4.1	4.5	4.1	4.5	17.2
6	Date-issued	4.3	4.4	4.3	4.2	17.2
16	Home-address	4.2	4.3	4.0	4.2	16.7
19	Low risk-to-security ratio	4.0	4.4	3.5	3.9	15.8
14	Gender	3.8	3.8	3.8	4.1	15.5
21	Tamper-proofing	4.3	3.4	3.8	3.8	15.3
2	Biometrics-simple	3.5	3.7	3.7	3.8	14.7
9	Document-electronics	2.9	4.1	3.5	4.1	14.6
5	Country of origin	3.4	3.5	3.3	3.5	13.7
1	Biometrics-advanced	1.2	4.0	1.6	3.9	10.7
10	Document-medium	2.6	2.1	2.7	2.4	9.8
12	employment-data	2.2	2.3	2.2	2.2	8.9
11	Document-size	1.9	1.5	2.3	1.5	7.2

Consensus	90%
	80%

Table 5. Synthesis of Results

This is an area where it seems very clear that further research is needed to explore this apparent expectation gap, to follow up on the research method described in this document, and

show how it could lead to making change recommendations in best practices, and/or mitigating procedures, and/or policies for major stakeholders: for example, the financial services regulatory bodies, and the financial institutions themselves. It would be interesting to explore, for example, what improvements could be made to the Federal Financial Institutions Examination Council (FFIEC) Examiners Manual for reviewing a bank's procedures related to preventing and detecting possible identity fraud during the opening of new accounts. Or more specifically, there may be benefits directly to a financial institution for mitigating fraud losses, if the expert procedures can be improved with regard to accepting identity documents presented when a customer opens a new account.

Limitations of the Research

One of the main limitations of this study is the limited statistical conclusion validity caused by the small sample size. This is offset to some extent by the use of the repertory grid interview technique, which typically does not require a large number of interviews. Recall that the method was originally developed for one-on-one therapy between a psychology counselor and client.

However, In this research situation where the participant expert rates the credibility attributes, the researcher's first stage in a process of creating a credibility index would be facilitated by a principal components analysis, using correlations among the attribute ratings to develop a small set of components that empirically summarizes these correlations (Tabachnick and Fidell, 2001). This method normally requires a minimum 100 data items (interviews), with an average 250-500 considered sufficient to give statistically valid results. However, (Mertler and Vannatta, 2001), suggest that these be considered general guidelines, not specific criteria to be met by the researcher. They go on to recommend using *Bartlett's Sphericity Test* for a factor

analysis with small sample sizes; a procedure that tests a null hypothesis that variables in the population correlation matrix are uncorrelated. Further commentary on this potential problem is provided by (Stevens, 1992); if this null hypothesis is rejected, there is no reason to do a principal components analysis, since the variables have already been shown to be uncorrelated.

Another limitation arises from the nature of the constructs elicited from the experts in round one. There may well be some overlap or interaction between these that would also interfere with the validity of any statistical conclusions to be derived. In addition, these constructs represent the expert knowledge. Research results concerning knowledge are shaped by the data available to the scholar for analysis (Ács and Audretsch, 2005)

Finally, there was the limitation of time on each of the round one interviews. Remember that a minimum of ten years experience was required of the interview participants. Typically, this level of experience is associated with mid-upper-level managers in a financial institution. Only the construct elicitation phase of the repertory grid method has been used. Requesting more time from busy managers would have resulted in a much lower level of participation. The full grid analysis is deferred for future research. Even during construct elicitation with twelve elements, only 25 of 220 (12 * 11 * 10 / 6) possible triads were used, again to limit the research interviews to approximately one hour in length.

IX. FUTURE RESEARCH

The possibilities are excellent for further research. In describing the research journey, it was suggested that the paths NOT taken along the way could provide pointers to future researchers for new discoveries. So a review of these untrodden paths seems appropriate here.

1. The broad domain for this research was limited to the financial services industry (banks and credit unions). The repertory grid methodology is extremely versatile. For example, if we consider experts in any other field, the method is applicable to tease out their constructs for their field related expertise. One area of growing interest is engaged scholarship, briefly mentioned in this document. It seems that the repertory grid approach could be used as a tool for engaged scholarship.

2. The specific activity where risk is highest is when opening a new account – this is the specific domain for this research.

3. Personnel selected as experts had a minimum of 10 years of experience. For the purpose of developing the credibility index, relaxing this requirement to 5 years, and expanding the geographical boundaries beyond southeast Florida would result in a much larger number of interviews. This would also be helpful in item 6 below.

4. Some additional boundaries were set in limiting the number of elements in the repertory grid (twelve identity documents). This seems to be a practical limit both from a repertory grid theory perspective, and from a time management perspective.

5. This research focuses only on financial identity fraud. With some thought, the application of this research can be seen to extend far beyond the domain of financial identity theft. Another example! Imagine if such a tool were available for evaluating different types of identity documents for international graduate school applicants.

6. Only the construct elicitation phase of the repertory grid method is used. Requesting more time from busy managers would have resulted in a much lower level of participation. However, follow-up interviews may be possible, and at the same time, additional managers could be interviewed, to develop the basis for a principal components analysis of credibility in identity documents.

7. During construct elicitation with twelve elements, only 25 of 1320 (12*11*10) possible triads were used, in order to limit the research interviews to approximately one hour in length. Again, longer interviews would have resulted in a much lower level of participation. This also seems to be a practical limit both from a repertory grid theory perspective, and from a time management perspective.

8. Although six significant trends were identified (for 36 possible scenarios), they were grouped in two sets of three, to limit the research to the use of four scenarios. The use of additional scenarios could provide finer granularity in understanding the impact that environment and context have on expert judgment.

And even beyond this, there are specific research threads that emerge. These are described in the following sections.

Calculus of Credibility

A further extension of these ideas can be developed, by creating a calculus of credibility, with a focus on individual documents rather than document types. As a start, the calculus would contain concepts for identity, policy, and organization. It would describe information protocols for what the identity document should contain, and action protocols for how the organization authenticates identity and provides affordances. The ideas can even be extended further to develop a logic-based description of identity fraud, with the goal of being able to describe a pattern matching approach to recognize the symptoms of potential identity fraud, and so prevent the crime from occurring.

Credibility Index

The participant ratings of the relative importance of each characteristic of credibility in the four different scenarios can be used as the basis for a composite credibility index for any existing identity document in any of the forecast scenarios, or even any new document that may emerge over time. As already suggested, expanding the sample size, to 300 or more, will provide a large enough data set to give reliable statistical results for principal components analysis or other methods of statistical inference. Further, the number of scenarios could be expanded, and the criteria for each scenario fine-tuned to provide indicators of how the credibility index would be affected by different trends in the financial services industry.

Qualitative and Quantitative Probability Networks

Another exciting possibility for future research is pictured in the drawing below. This research has assumed that each type of identity document is independent of the others. Again, in real life this is not so.

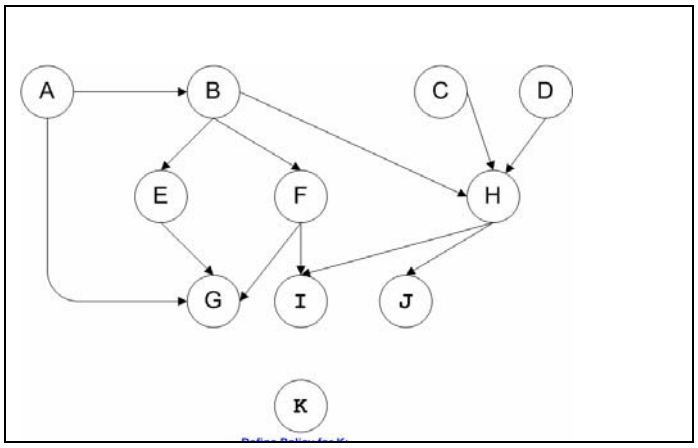

Figure 11. Inter-organizational Evidence Flow Network

As seen in Figure 12, Organization H has a policy requiring three types of identity documents, from B, C, and D. Similarly, *prima facie*, Organization G has a policy requiring three types of identity documents, from A, E, and F. However, these policies are not similar at all. In fact, we can see from the picture that G really is depending only on A to have made a good decision about issuing its identity documents, given that both E and F ultimately are also placing their trust in A. Because identity documents are ***not*** all equal, it would be useful to be able to calculate the joint probability that each document is credible. Now the question is, what policy should Organization K adopt for its new account identity document requirements?

Inter-Organizational Evidence Flow

There are exciting possibilities for additional research in this area. Although the context of an inter-organizational environment has been discussed, it is clear that the goal for this research is to measure the credibility index only for individual document types, and only in the environment of a single organization. However, real life is not so simplistic. First, the identity document creation and verification process is very much inter-organizational, as each organization reviews, and decides whether or not to accept, the documents created by other organizations. In so doing, each organization sets an implicit policy about the credibility of identity documents created by specific other organizations. ***This may not be a good policy***.

We can imagine an identity fraud chain among organizations (Org) that rely on evidence in the form of identity documents created by another Org. Suppose Org(0) requires a birth certificate;

- each subsequent Org(n) depends on the prior Org(n-1) in the chain.
- i.e., Org(1) needs evidence(1) from Org(0), and
- and Org(2) needs evidence(2) from Org(1)

- . . .

- and Org(j) needs evidence(j) from Org(j-1)

The deception begins if any Org(k) incorrectly validates evidence(k), based on a successful lie by a perpetrator who never in fact received evidence(k) from Org(k-1). And now the deception gains strength with each link, as the perpetrator submits evidence(k) to Org(k+1) and so on.

BIBLIOGRAPHY

Abels, E. G., White, M. D., and Hahn, K. "Identifying User-Based Criteria for Web Pages." *Internet Research* 7, no. 4 (1997): 252-262.

Ács, Z., and Audretsch, D. *Handbook of Entrepreneurship Research: An Interdisciplinary Survey and Introduction*. New York, NY: Springer Verlag, (2005).

Alexander, J. E., and Tate, M. A. *Web Wisdom: How to Evaluate and Create Information Quality on the Web*. Mahwah, NJ: Lawrence Erlbaum Associates, (1999).

Andrews, L. W., and Gutkin, T. B. "The Effects of Human Versus Computer Authorship on Consumers' Perceptions of Psychological Reports." *Computers in Human Behavior* 7, no. 4 (1991): 311-317.

Aristotle. *On Rhetoric: A Theory of Civic Discourse*. Translated by Kennedy, G. A. New York, NY: Oxford University Press, (1991 translation).

Barrett, D. *Busboy Admits Stealing Identities of America's Rich and Famous*. October 3 (2002), Associated Press Newswires, accessed June 25, 2007; Available from http://www.radicus.net/news/listall/tw.top.asp.

Barry, C. L. "User-Defined Relevance Criteria: An Exploratory Study." *Journal of the American Society for Information Science* 45, no. 3 (1994): 149-159.

Barry, Carol, and Schamber, Linda. "Users' Criteria for Relevance Evaluation: A Cross-Situational Comparison." *Information Processing & Management* 34, no. 2-3 (1998): 219-236.

Bateman, Judith Ann. "Modeling Changes in End-User Relevance Criteria : An Information Seeking Study." Dissertation, University of North Texas, (1998).

Bell, D. E. "Potential Contributions to Decision Analysis." *Decision Sciences* 13, no. 4 (1982): 534-540.

Better Business Bureau. *New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think*. (2006), accessed 07/07/2006, http://www.bbbonline.org/idtheft/safetyQuiz.asp.

Bowron, Mike, and Shaw, Oliver. "Fighting Financial Crime: A UK Perspective." *Economic Affairs* 27, no. 1 (2007): 6-9.

Burbules, N. C. "Paradoxes of the Web: The Ethical Dimensions of Credibility." *Library Trends* 49, no. 3 (2001): 441-453.

Cabrera, D. A. "Boundary Critique: A Minimal Concept Theory of Systems Thinking." In *50th Annual Meeting of the ISSS*, (2006).

Canadian Consumer Measures Committee. *Working Together to Prevent Identity Theft*. (2005).

CERT. *Overview of Attack Trends,* . (2002), Pittsburgh, Pennsylvania: CERT Coordination Center, accessed June 25, 2007; Available from www.cert.org/archive/pdf/attack_trends.pdf.

Chermack, T. J., van der Merwe, L., and Lynham, S. A. "Exploring the Relationship between Scenario Planning and Perceptions of Strategic Conversation Quality." *Technological Forecasting and Social Change* 74, no. 3 (2007): 379-390.

Collins, J. M. "Business Identity Theft." *Journal of Forensic Accounting* 4, no. 2 (2003): 303-306.

ConsumerAffairs.com. *"Vishing" Is Latest Twist in Identity Theft Scam,* . July 24 (2006), accessed June 25, 2007; Available from http://www.consumeraffairs.com/news04/2006/07/scam_vishing.html.

Cooke, Alison. *Neal-Schuman Authoritative Guide to Evaluating Information on the Internet*. Neal-Schuman Netguide Series. New York: Neal-Schuman Publishers, (1999).

Cool, C., Belkin, N. J., and Kantor, P. B. "Characteristics of Texts Affecting Relevance Judgments." In *Proceedings of the 14th National Online Meeting*, 77–84, (1993).

Copernicus, Nicolas. "Minor Works: Meditata (Private Reflections)." In *Nicolas Copernicus: Complete works*, ed. Czartoryski, Pawel, 3. London, England: The Macmillan Press, (1517).

Darby, M. R., and Karni, E. "Free Competition and the Optimal Amount of Fraud." *Journal of Law and Economics* 16, no. 1 (1973): 67-88.

Darley, W. K., and Smith, R. E. "Advertising Claim Objectivity: Antecedents and Effects." *Journal of Marketing* 57, no. 4 (1993): 100-113.

Dateline-NBC. "Passport Investigation Suggests Security Hole." ed. Stone Phillips, Richard Greenberg, Adam Ciralsky. USA, (2007).

Davis, C. J., Fuller, R. M., Tremblay, M. C., and Berndt, D. J. "Communication Challenges in Requirements Elicitation and the Use of the Repertory Grid Technique." *JOURNAL OF COMPUTER INFORMATION SYSTEMS* 46, no. 5 (2006): 78.

Davis, C. J., and Hufnagel, E. M. "Through the Eyes of Experts: A Socio-Cognitive Perspective on the Automation of Fingerprint Work." *MANAGEMENT INFORMATION SYSTEMS QUARTERLY* 31, no. 4 (2007): 681.

Davis, E., Kay, J., and Star, J. "Is Advertising Rational." *Business Strategy Review* 2, no. 3 (1991): 1-23.

Davis, Kristin. "Targeting Kids for Identity Theft." *Kiplinger's Personal Finance Magazine*, January 2004, 20.

Diewert, W. E., and Nakamura, A. *Essays in Index Number Theory*. Edited by Jorgenson, D.W., Laffont, J.J. and Persson, T. Vol. 1, Contributions to Economic Analysis. Amsterdam, The Netherlands: Elsevier Science Publishers, (1993).

Dijkstra, Jaap J. "User Agreement with Incorrect Expert System Advice." *Behaviour & Information Technology* 18, no. 6 (1999): 399 - 411.

Dijkstra, Jaap J., Liebrand, Wim B. G., and Timminga, Ellen. "Persuasiveness of Expert Systems." *Behaviour & Information Technology* 17, no. 3 (1998): 155 - 163.

Dixon, Pam *Medical Identity Theft: The Information Crime That Can Kill You*. May 3 (2006), "World Privacy Forum", accessed June 24, 2007; Available from http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.

Donath, J. S. *Identity and Deception in the Virtual Community*. Edited by Kollock, P. and Smith, M. Vol., Communities in Cyberspace. London, England: Routledge, (1999).

Dragulanescu, N. "Website Quality Evaluations: Criteria and Tools." *The International Information & Library Review* 34 (2002): 247-254.

The Fair and Accurate Credit Transactions Act, (2003). 15 U.S.C. § 1681 et seq. P.L. 108-159

FBI. *No Ordinary Case of Identity Theft*. October 18 (2004), Federal Bureau of Investigation, accessed July 15, 2006; Available from http://www.fbi.gov/page2/oct04/uncoveridt101504.htm.

Federal Deposit Insurance Corporation. *Legislative and Regulatory Responses to Identity Theft* December 10 (2004), "Putting an End to Account-Hijacking Identity Theft ", accessed June 24, 2007; Available from http://www.fdic.gov/consumers/consumer/idtheftstudy/legislative.html#fn51.

Fisher, D. "Group Fights Online ID Theft." In *eWeek*, 22, (2003).

Fisher, I. *The Making of Index Numbers: A Study of Their Varieties, Tests, and Reliability*. 1 ed. New York, New York: Houghton Mifflin company, (1922).

Flanagin, Andrew J., and Metzger, Miriam J. "The Perceived Credibility of Personal Web Page Information as Influenced by the Sex of the Source." *Computers in Human Behavior* 19, no. 6 (2003): 683-701.

Florida, Sixteenth Statewide Grand Jury. (2002) *Statewide Grand Jury Report: Identity Theft in Florida.* First Interim Report of the Sixteenth Statewide Grand Jury

Fogg, B. J. "Prominence-Interpretation Theory: Explaining How People Assess Credibility Online." In *CHI '03 extended abstracts on Human factors in computing systems*. Fort Lauderdale, Florida: ACM Press, (2003).

Fogg, B. J., Marshall, J., Kameda, T., Solomon, J., Rangnekar, A., Boyd, J., and Brown, B. "Web Credibility Research: A Method for Online Experiments and Early Study Results." *Conference on Human Factors in Computing Systems* (2001): 295-296.

Fogg, B. J., Swani, P., Treinen, M., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., Paul, J., and Rangnekar, A. "What Makes Web Sites Credible?: A Report on a Large Quantitative Study." In *Proceedings of the SIGCHI conference on Human factors in computing systems*, 61-68, (2001).

Fogg, B. J., and Tseng, H. "The Elements of Computer Credibility." In *Proceedings of the SIGCHI conference on Human factors in computing systems: the CHI is the limit*, 80-87, (1999).

Foley, Linda, and Foley, Jay. *Identity Theft: The Aftermath 2003*. (2003), "Identity Theft Resource Center", accessed June 3, 2007, http://www.idtheftcenter.org/artman2/uploads/1/The_Aftermath_2003.pdf.

Ford, D. N., and Sterman, J. D. "Expert Knowledge Elicitation to Improve Formal and Mental Models." *System Dynamics Review* 14, no. 4 (1998): 309-340.

Ford, G. T., Smith, D. B., and Swasy, J. L. "Consumer Skepticism of Advertising Claims: Testing Hypotheses from Economics of Information." *The Journal of Consumer Research* 16, no. 4 (1990): 433-441.

Fragale, A. R., and Heath, C. "Evolving Informational Credentials: The (Mis) Attribution of Believable Facts to Credible Sources." *Personality and Social Psychology Bulletin* 30, no. 2 (2004): 225.

Fransella, F., and Bannister, D. *A Manual for Repertory Grid Technique*. New York, New York: Academic Press, (1977).

Fransella, F., Bannister, D., and Bell, R. *A Manual for Repertory Grid Technique*. 2nd ed. Chichester, West Sussex, England: John Wiley and Sons Ltd., (2004).

Fritch, J. W., and Cromwell, R. L. "Evaluating Internet Resources: Identity, Affiliation, and Cognitive Authority in a Networked World." *Journal of the American Society for Information Science and Technology* 52, no. 6 (2001): 499-507.

GAO. (1998) *Identity Fraud: Information on Prevalence, Cost, and Internet Impact Is Limited.* Stana, Richard M.; Burton, Danny R. Briefing Report to Congressional Requesters [GAO/GGD-98-100BR]

GAO. (2002a) *Identity Fraud: Prevalence and Links to Alien Illegal Activities.* Stana, Richard M. Before the Subcommittee on Crime, Terrorism and Homeland Security and the Subcommittee on Immigration, Border Security, and Claims, Committee on the Judiciary, House of Representatives [GAO-02-830T] http://www.gao.gov/new.items/d02830t.pdf

GAO. (2002b) *Identity Theft: Available Data Indicate Growth in Prevalence and Cost.* Stana, Richard M.; Burton, Danny R. Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate [GAO-02-424T] http://www.gao.gov/new.items/d02424t.pdf

GAO. (2002c) *Identity Theft: Greater Awareness and Use of Existing Data Are Needed.* Stana, Richard M.; Burton, Danny R. Report to the Honorable Sam Johnson House of Representatives [GAO-02-766] http://www.gao.gov/new.items/d02766.pdf

GAO. (2002d) *Identity Theft: Prevalence and Cost Appear to Be Growing.* Stana, Richard M.; Burton, Danny R. Report to Congressional Requesters [GAO-02-363] http://www.gao.gov/new.items/d02363.pdf

GAO. (2005) *Improvements Needed to Strengthen Us Passport Fraud Detection Efforts.* Ford, J.T. Testimony Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate [GAO-05-853T] http://www.gao.gov/new.items/d05853t.pdf

Goldberg, M. E., and Hartwick, J. "The Effects of Advertiser Reputation and Extremity of Advertising Claim on Advertising Effectiveness." *The Journal of Consumer Research* 17, no. 2 (1990): 172-179.

Gonzales, Alberto R. (2007) *Combating Identity Theft: A Strategic Plan.* [Volume 1] http://www.idtheft.gov/reports/StrategicPlan.pdf

Gregor, S., and Benbasat, I. "Explanations from Intelligent Systems: Theoretical Foundations and Implications for Practice." *MIS Quarterly* 23, no. 4 (1999): 497-530.

Hevner, A. R., March, S. T., Park, J., and Ram, S. "Design Science in Information Systems Research." *MIS Quarterly* 28, no. 1 (2004): 75-105.

Heyer, R. (2004) *Understanding Soft Operations Research: The Methods, Their Application and Its Future in the Defence Setting.* DSTO Information Sciences Laboratory. [DSTO-GD-0411] http://www.dsto.defence.gov.au/publications/3451/DSTO-GD-0411.pdf

Hinkle, D. N. "The Change of Personal Constructs from the Viewpoint of a Theory of Implications, 1965." Unpublished PhD thesis, Columbus, OH.

Hinkle, D. N. *The Game of Personal Constructs*. Edited by Bannister, D. Vol., Perspectives in Personal Construct Theory. London, England: Academic Press, (1970).

Hogarth, R. M. *Judgment and Choice: The Psychology of Decision*. 2nd ed.: John Wiley & Sons, (1996).

Holbrook, M. B. "Beyond Attitude Structure: Toward the Informational Determinants of Attitude." *Journal of Marketing Research* 15, no. 4 (1978): 545-556.

Hovland, C. I., Janis, I. L., and Kelley, H. H. *Communication and Persuasion: Psychological Studies of Opinion Change*. New Haven, CT: Yale University Press, (1953).

Hovland, C. I., and Weiss, W. "The Influence of Source Credibility on Communication Effectiveness." *The Public Opinion Quarterly* 15, no. 4 (1951): 635-650.

Howard, Heather M. "The Negligent Enablement of Imposter Fraud: A Common–Sense Common Law Claim." *DUKE LAW JOURNAL* 54, no. 5 (2005): 1266.

Hufnagel, E. M., and Conca, C. "User Response Data: The Potential for Errors and Biases." *Information Systems Research* 5, no. 1 (1994): 48-73.

Huss, W. R. "A Move Towards Scenarios." *International Journal of Forecasting* 4 (1988): 377-388.

Identity Theft and Assumption Deterrence Act (1998). 18 U.S.C. § 1028(d)(7). 105-318.

Infante, D. A., Parker, K. R., Clarke, C. H., Wilson, L., and Nathu, I. A. "A Comparison of Factor and Functional Approaches to Source Credibility." *Communication Quarterly* 31, no. 1 (1983): 43–48.

Internet False Identification Act (2000). 18 U.S.C § 1001, § 1028. P.L. 106-578.

Janes, J. W., and Rosenfeld, L. B. "Networked Information Retrieval and Organization: Issues and Questions." *Journal of the American Society for Information Science* 47, no. 9 (1996): 711-715.

Jankowicz, D. *The Easy Guide to Repertory Grids*. Chichester, West Sussex, England: John Wiley and Sons Ltd., (2003).

Javelin. *New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think*. (2006), "Javelin Strategy and Research", San Francisco, CA: Better Business Bureau, accessed July 7, 2006, http://www.bbb.org/Alerts/article.asp?ID=651.

Javelin, Strategy & Research. *2007 Identity Fraud Report—Consumer Version: How Consumers Can Protect Themselves*. February (2007), Pleasanton, CA: accessed March 29, 2007; Available from http://www.freakonomics.com/pdf/Javelin%20Report%202007.pdf.

Johnson, T. J., and Kaye, B. K. "Cruising Is Believing? Comparing Internet and Traditional Sources on Media Credibility Measures." *Journalism & Mass Communication Quarterly* 75, no. 2 (1998): 325-340.

Johnson, T. J., and Kaye, B. K. "Using Is Believing: The Influence of Reliance on the Credibility of Online Political Information among Politically Interested Internet Users." *Journalism & Mass Communication Quarterly* 77, no. 4 (2000): 865-879.

Johnson, T. J., and Kaye, B. K. "Webelievability: A Path Model Examining How Convenience and Reliance Predict Online Credibility." *Journalism & Mass Communication Quarterly* 79, no. 3 (2002): 619-642.

Kelly, G. *The Psychology of Personal Constructs I and I.I*. New York: WW Norton, (1955).

Kelly, G. A. "The Function of Interpretation in Psychotherapy. A Series of Three Lectures Given to Los Angeles Society of Clinical Psychologists in Private Practice, 1959." London: Centre for Personal Construct Psychology, (1959).

Kelly, G. A. "The Role of Classification in Personality Theory." In *Clinical Psychology and Personality*, ed. Maher, B., 1979, 289-300. Huntington, New York: Robert E. Krieger Publishing Company, (1965).

Kelly, G. A. "The Function of Interpretation in Psychotherapy. A Series of Three Lectures Given to Los Angeles Society of Clinical Psychologists in Private Practice, 1959." London: Centre for Personal Construct Psychology, (1989).

Kelly, G. A. *The Psychology of Personal Constructs*. Routledge, (1992).

Kiousis, S. "Public Trust or Mistrust? Perceptions of Media Credibility in the Information Age." *Mass Communication & Society* 4, no. 4 (2001): 381-403.

Kjartansdóttir, A., and Widenius, M. "The Quality of Business Information on the Internet: Evaluation Criteria Applicable to Internet Resources." *Swedish Library Research* 3, no. 4 (1995a): 43–50.

Kjartansdóttir, A., and Widenius, M. "The Quality of Business Information on the Internet: Evaluation Criteria Applicable to Internet Resources." *Swedish Library Research* 3, no. 4 (1995b): 43-50.

Koester, R., and Luthans, F. "The Impact of the Computer on the Choice Activity of Decision Makers: A Replication with Actual Users of Computerized Mis." *The Academy of Management Journal* 22, no. 2 (1979): 416-422.

Krantz, D. H., Luce, R. D., Suppes, P., and Tversky, A. *Foundations of Measurement*. 1. New York: Academic. New York, New York: Academic Press, (1971).

Landfield, A. W. *Personal Construct Systems in Psychotherapy*. Chicago, IL: Rand McNally, (1971).

Lee, Jennifer. "Identity Theft Victimizes Millions, Costs Billions." *New York Times*, September 4, 2003 (2003).

Leland, John. "Some ID Theft Is Not for Profit, but to Get a Job." *New York Times*, September 4 (2006).

Lerch, F. J., Prietula, M. J., and Kulik, C. T. *The Turing Effect: The Nature of Trust in Expert Systems Advice*. Edited by Feltovich, Paul J., Ford, Kenneth M. and Hoffman, Robert R. Vol., Expertise in Context: Human and Machine Table of Contents. Cambridge, MA: MIT Press, (1997).

Liu, Z. "Perceptions of Credibility of Scholarly Information on the Web." *Information Processing and Management: an International Journal* 40, no. 6 (2004): 1027-1038.

Locke, K., Golden-Biddle, K., Edmonton, A., and Feldman, M. S. "Imaginative Theorizing in Organizational Research." In *American Political Science Association Annual Meeting*. Chicago, IL (2004).

Luthans, F., and Koester, R. "The Impact of Computer Generated Information on the Choice Activity of Decision-Makers." *The Academy of Management Journal* 19, no. 2 (1976): 328-332.

Maglaughlin, Kelly L., and Sonnenwald, Diane H. "User Perspectives on Relevance Criteria: A Comparison among Relevant, Partially Relevant, and Not-Relevant Judgments." *Journal of the American Society for Information Science and Technology* 53, no. 5 (2002): 327-342.

Marsh, S., and Dibben, M. R. "The Role of Trust in Information Science and Technology." *Annual Review of Information Science and Technology* 37, no. 1 (2003): 465-498.

McCroskey, J. C., and Young, T. J. "Ethos and Credibility: The Construct and Its Measurement after Three Decades." *Central States Speech Journal* 32 (1981): 24-34.

Mertler, Craig A., and Vannatta, Rachel A. *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation*. Los Angeles, California: Pyrczak Publishing, (2001).

Metzger, Miriam J., Flanagin, Andrew J., and Zwarun, Lara. "College Student Web Use, Perceptions of Information Credibility, and Verification Behavior." *Computers & Education* 41, no. 3 (2003): 271-290.

Meyer, P. "Defining and Measuring Credibility of Newspapers: Developing an Index." *Journalism Quarterly* 65, no. 3 (1988): 567-574.

Mihm, Stephen. "Dumpster-Diving for Your Identity." *The New York Times Magazine*, December 21 2003, 42.

Miles, I. , Green, L., and Popper, R. *Scenario Methodology for Ist Foresight in the European Research Area*. Foresight on Information Society Technologies in the European Research Area (FISTERA), (2004).

Muir, B. M. "Trust between Humans and Machines, and the Design of Decision Aids." *International Journal of Man-Machine Studies* 27, no. 5-6 (1987): 527-539.

Murphy, David S. "Auditor Evidence Evaluation: Expert Systems as Credible Sources." *Behaviour & Information Technology* 15, no. 1 (1996): 14 - 23.

Nass, C., and Mason, L. "On the Study of Technology and Task: A Variable-Based Approach." In *Organizations and Communication Technology*, ed. Fulk, J. and Steinfeld, C., 46-67. Newbury Park, CA: Sage, (1990).

Nelson, P. "Advertising as Information." *The Journal of Political Economy* 82, no. 4 (1974): 729-754.

Newhagen, J., and Nass, C. "Differential Criteria for Evaluating Credibility of Newspapers and Tv News." *Journalism Quarterly* 66, no. 2 (1989): 277-284.

Newman, Graeme R., and McNally, Megan M. *Identity Theft Literature Review*. U.S. Department of Justice (2005).

Nicolae-George, D. "Website Quality Evaluations: Criteria and Tools." *The International Information and Library Review* 34, no. 2 (2002): 247–254.

O'Brien, Timothy L. . "Gone in 60 Seconds." *New York Times*, October 24 (2004).

Olaisen, J. *Information Quality Factors and the Cognitive Authority of Electronic Information*. Edited by Wormell, I. Vol., Information Quality: Definitions and Dimensions. Los Angeles, CA: Taylor Graham, (1990).

Pancer, S. M. "Understanding and Predicting Attitudes Towards Computers." *Computers in Human Behavior* 8 (1992): 211-222.

Park, Taemin Kim. "The Nature of Relevance in Information Retrieval: An Empirical Study." Ph.D., Indiana University, (1992).

Paul, Sara R. *Features - Identity Theft: Outline of Federal Statutes and Bibliography of Select Resources*. February 7 (2007), "New York City District Attorney's Office", New York, NY: accessed June 24, 2007, http://www.llrx.com/features/idtheftguide.htm#id%20theft%20statutes.

Peiling Wang, Dagobert Soergel. "A Cognitive Model of Document Use During a Research Project. Study I. Document Selection." *Journal of the American Society for Information Science* 49, no. 2 (1998): 115-133.

Petty, R. E., and Cacioppo, J. T. *Attitudes and Persuasion: Classic & Contemporary Approaches*. Westview Press, (1986).

Polanyi, M. *The Tacit Dimension*. Edited by Smith, Peter. Vol., Knowledge in Organizations. Gloucester, MA, (1966).

Porter, M. E. *Competitive Advantage*. New York, NY: Free Press New York, (1985).

Pratt, G. F., Flannery, P., and Perkins, C. L. D. "Guidelines for Internet Resource Selection." *College & research libraries news* 57, no. 3 (1996): 134-135.

Quinn, Jennifer Viola. "A Measurement of Credibility in the Forensics Realm." M.A., California State University, Fullerton, (2004).

Raubitschek, R. S. "Multiple Scenario Analysis and Business Planning." *Advances in Strategic Management* 5 (1988): 181–205.

Reeves, B., and Nass, C. *The Media Equation: How People Treat Computers, Television, and New Media Like Real People and Places*. New York, NY: Cambridge University Press (1996).

Rieh, S. Y. "Information Quality and Cognitive Authority in the World Wide Web." Dissertation, Rutgers, (2000).

Rieh, S. Y. "Judgment of Information Quality and Cognitive Authority in the Web." *Journal of the American Society for Information Science and Technology* 53, no. 2 (2002): 145-161.

Rieh, S. Y., and Belkin, N. J. "Understanding Judgment of Information Quality and Cognitive Authority in the Www." In *Proceedings of the ASIS Annual Meeting*, 35, 279-289, (1998).

Roberts, F. S. "Measurement Theory, with Applications to Decisionmaking, Utility, and the Social Sciences." In *Encyclopedia of Mathematics and Its Applications*, ed. Rota, Gian-Carlo, 7. Reading, Massachusetts: Addison-Wesley Publishing Company, (1979).

Rogers, E. M. *Diffusion of Innovation*. Vol. New York, NY: The Free Press New York, (1995).

Roper, B. W. *Public Attitudes toward Television and Other Media in a Time of Change: The Fourteenth Report in a Series*. Roper Organization - Television Information Office, (1985).

Ruona, W. E. A., and Lynham, S. A. "A Philosophical Framework for Thought and Practice in Human Resource Development." *Human Resource Development International* 7, no. 2 (2004): 151-164.

Rusch, Jonathan J. . *Making a Federal Case of Identity Theft: The Department of Justice's Role in Identity Theft Enforcement and Prevention*. July (2001), accessed June 24, 2007; Available from http://fbilibrary.fbiacademy.edu/bibliographies/identitytheft.htm.

Saracevic, Tefko. "Relevance Reconsidered." In *Conceptions of Library and Information Science* Copenhagen (Denmark), (1996).

Schamber, L., and Bateman, J. "User Criteria in Relevance Evaluation: Toward Development of a Measurement Scale." In *Proceedings of the American Society for Information Science, Baltimore, MD*, 218–225, (1996).

Schoemaker, P. J. H. "Multiple Scenario Development: Its Conceptual and Behavioral Foundation." *Strategic Management Journal* 14, no. 3 (1993): 193-213.

Schwartz, P. *The Art of the Long View*. New York, NY: Doubleday, (1991).

Singletary, M. W. "Components of Credibility of a Favorable News Source." *Journalism Quarterly* 53, no. 1976 (1976): 316-319.

Slater, M. D., and Rouner, D. "How Message Evaluation and Source Attributes May Influence Credibility Assessment and Belief Change." *Journalism and Mass Communication Quarterly* 73, no. 4 (1996): 974-91.

Social Security Number Confidentiality Act (2000). 31 U.S.C. § 3327. P.L. 106-433.

Stefano, Mizzaro. "Relevance: The Whole History." *Journal of the American Society for Information Science* 48, no. 9 (1997): 810-832.

Stevens, J. P. *Applied Multivariate Statistics for the Social Sciences (2nd Ed.)*. Hillsdale, NJ: Lawrence Erlbaum Associates, (1992).

Stewart, V., Stewart, A., and Fonda, N. *Business Applications of Repertory Grid*. Maidenhead, Berkshire, England: McGraw-Hill Book Company (UK) Limited, (1981).

Sullivan, Bob. *Fake Companies, Real Money: Elaborate Con Wrings Cash out of Stolen Credit Cards*. October 7 (2004), accessed June 25, 2007; Available from http://www.msnbc.msn.com/id/6175738.

Swartz, N. "Want the CIA Director's Address? Get It for $26 Online.(up Front: News, Trends &Amp; Analysis)." *The information management journal* 37, no. 6 (2003): 16(1).

Swinney, L. "Consideration of the Social Context of Auditors' Reliance on Expert System Output During Evaluation of Loan Loss Reserves." *International Journal of Intelligent Systems in Accounting Finance & Management* 8, no. 3 (1999): 199-213.

Tabachnick, B. G., and Fidell, L. S. *Using Multivariate Statistics*. Needham Heights, Massachusetts: Allyn & Bacon, (2001).

Taylor, R. S. *Value-Added Processes in Information Systems*. Edited by Voigt, Melvin J. Vol. Westport, CT: Greenwood Publishing Group Inc., (1986).

Thorndike, L. "Vatican Latin Manuscripts in the History of Science and Medicine." *Isis* 13, no. 1 (1929): 53-102.

Towle, H. K. "Identity Theft: Myths, Methods, and New Law." *RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL* 30, no. 2 (2004): 242.

Tseng, S., and Fogg, B. J. "Credibility and Computing Technology." *Communications of the ACM* 42, no. 5 (1999): 39-44.

United States Department of Justice. *Identity Theft and Identity Fraud*. (2007), accessed June 24, 2007, http://www.usdoj.gov/criminal/fraud/websites/idtheft.html.

USDOJ. *Identity Theft and Identity Fraud*. (2007), "US Department of Justice", accessed June 3, 2007, http://www.usdoj.gov/criminal/fraud/websites/idtheft.html.

Van de Ven, Andrew H. *Engaged Scholarship: A Guide for Organizational and Social Research*. New York, NY: Oxford University Press, (2007).

Vandenbergh, B. G., Soley, L. C., and Reid, L. N. "Factor Study of Dimensions of Advertiser Credibility." *Journalism Quarterly* 58, no. 4 (1981): 629-632.

Vijayan, J. "Firms Unite to Fight Online ID Theft." *Computerworld*, 2003, 36-51.

Vogt, Arthur, and Barta, Janos. *The Making of Tests for Index Numbers: Mathematical Methods of Descriptive Statistics*. Heidelberg, Germany: Springer-Verlag, (1997).

Wack, P. "Scenarios: Shooting the Rapids." *Harvard Business Review* 63, no. 6 (1985): 139-150.

Wærn, Y., and Ramberg, R. "People's Perception of Human and Computer Advice." *Computers in Human behaviour* 12 (1996).

Walsh, J. P. "Managerial and Organizational Cognition: Notes from a Trip Down Memory Lane." *Organization Science* 6, no. 3 (1995): 280-321.

Wang, G., Chen, H., and Atabakhsh, H. "Automatically Detecting Deceptive Criminal Identities." *Communications of the ACM* 47, no. 3 (2004): 70-76.

Wang, P. "The Design of Document Retrieval Systems for Academic Users: Implications of Students on Users' Relevance Criteria." *Proceedings of the ASIS Annual Meeting* 34 (1997): p162-73.

Wang, P., and Domas-White, M. "A Cognitive Model of Document Use During a Research Project. Study II. Decisions at the Reading and Citing Stages." *Journal of the American Society for Information Science* 50, no. 2 (1999): 98-114.

Wang, P., and Soergel, D. "A Cognitive Model of Document Use During a Research Project. Study I. Document Selection." *Journal of the American Society for Information Science* 49, no. 2 (1998): 115-133.

Wathen, C. N., and Burkell, J. "Believe It or Not: Factors Influencing Credibility on the Web." *Journal of the American Society for Information Science and Technology* 53, no. 2 (2002): 134-144.

Watson, J. S. "“If You Don't Have It, You Can't Find It.” a Close Look at Students' Perceptions of Using Technology." *Journal of the American Society for Information Science* 49, no. 11 (1998): 1024-1036.

White, M. D., Abels, E. G., and Hahn, K. "User-Based Design Process for Web Sites." *Internet Research* 8, no. 1 (1998): 39-50.

Widmeyer, G. R. "Preference Directed Reasoning in Decision Support Systems." Dissertation, University of Texas at Austin, (1986).

wikipedia.org. *Personal Construct Psychology*. June 19, 2007 (2007a), accessed http://en.wikipedia.org/wiki/Personal_construct_psychology.

wikipedia.org. *Scenario Planning*. (2007b), accessed August 31, 2007, http://en.wikipedia.org/wiki/Scenario_planning.

Willox Jr., Norman A. , Gordon, Gary R. , Regan, Thomas M. , Rebovich, Donald J. , and Gordon, Judith B. . "Identity Fraud: A Critical National and Global Threat." *Journal of Economic Crime Management* 2, no. 1 (2004).

Willox Jr., Norman A. , and Regan Esq., Thomas M. . "Identity Fraud: Searching for a Solution." In *White Paper*: Lexis-Nexis, (2001).

Wilson, P. *Second-Hand Knowledge: An Inquiry into Cognitive Authority*. Greenwood Press, (1983).

Ye, L. R., and Johnson, P. E. "The Impact of Explanation Facilities on User Acceptance of Expert Systems Advice." *MIS Quarterly* 19, no. 2 (1995): 157-172.

Zdanowicz, J. S. "Detecting Money Laundering and Terrorist Financing Via Data Mining." *Communications of the ACM* 47, no. 5 (2004): 53-55.

APPENDICES

Appendix 1 - Repertory Grid Interview Script

"The purpose of this interview is to help me understand, from your experience, what are the characteristics of identity document types that make those document types credible. Now I know there are compliance and security related lists of certain things you must look for on identity documents, but this is not what interests me. I want to get at your "*gut reaction*" - what makes you feel instinctively that there may be a problem with any identity document that you review. I will show you three types of identity document, and ask you to tell me what characteristic makes two of the three most similar, and how the third is different. We will repeat the process a number of times, using a different set of three document types each time. Sometimes, I may ask you to explain more details of the characteristics you named, to help me get a correct understanding of what you are telling me, as I will make notes of these characteristics and details you give me. Similarly, please ask me to explain any question I ask, if you are unsure what I mean. This repetition will continue for about one hour. At the end of the interview, I will ask you a couple of closing questions, and then we will be finished."

Appendix Two - Scenario Evaluation Interview Script

The top half of the page contains a composite list of 21 items, developed from the first round of interviews. These items describe the characteristics of identity documents that seem to make them credible for persons like you who have extensive experience with reviewing identity documents and evaluating their credibility. These characteristics are mostly self-explanatory, but some do require additional discussion that I will give you now. Then as we proceed, please ask any other questions that come to your mind.

- Biometrics-simple. These include picture, signature, height, weight, eye color, etc.

- Biometrics-advanced. These include DNA information, retinal scans, fingerprints, etc.

- Coded ID number. All identity documents have a unique numbers, but some numbers contain coded information. For example the first three digits of the Social Security number indicate the state where the number was issued. Similarly, the Florida drivers' license number includes information about gender, day of the month the holder was born, and so on.

- Authentication (database). This is an external characteristic, where a database of identity documents from the outside exists to authenticate the data on an ID document presented.

- Risk-to-security low ratio. A high ratio means:

There is a high risk exposure associated with successfully presenting a fraudulent identity document, while security features on the document are at a relatively low level, resulting in a high risk to security ratio.

I will describe four scenarios in the context of a customer opening a new account. You will recall that my research focuses on identity documents presented when a customer opens a new account. This is a high-risk activity for your organization, as you do not yet know your customer, and you have no basis to assess the accuracy of any assertions they make. For each of

the four scenarios, I will ask you to evaluate the importance of each one of the twenty-one characteristics, using the following evaluation question for each characteristic.

> "*As you visualize the given scenario, how important is it that the characteristic be present on the identity document being presented? Use a scale of 1 to 5, where: 1= no importance whatsoever; 5=critically important.*"

Here is the first scenario. It most closely reflects the current situation. The identity document:

- Could be issued by any third party – government, employer, insurance company, etc.
- Data includes a photo and signature.
- Is plastic or laminated, and about the size of a credit card
- Data can be authenticated, but offline; needs about 24-48 hours.
- Has little or no biometrics, little or no electronics.
- The customer must be physically present when opening the new account.

> "*As you visualize this first scenario, how important is it that each characteristic be present on the identity document being presented? Use a scale of 1 to 5, where: 1= no importance whatsoever, or not applicable; 5=critically important.*"

Here is the second scenario. The identity document:

- Could be issued by any third party – government, employer, insurance company, etc.
- Data includes a photo and signature.
- Is plastic or laminated, and about the size of a credit card
- Data can be authenticated, but offline; needs about 24-48 hours.
- Contains advanced biometrics (for example, DNA, retinal scans, fingerprints)
- Contains advanced electronics (RFID chip contains electronic form of all data, and it is continuously transmitting, so that the identity document can be tracked at all times)

- Is digital, not physical

- The customer is virtual, need not be physically present when opening the new account.

> "*As you visualize this second scenario, how important is it that each characteristic be present on the identity document being presented? Use a scale of 1 to 5, where: 1= no importance whatsoever, or not applicable; 5=critically important*."

Here is the third scenario. The identity document:

- Is legally issued only by a single centralized agency that could be either a government or private organization.

- Is issued by a process that can be trusted to ensure that the data accurately represents the applicant at the time of issue, and that the document is tamperproof.

- Data can be authenticated on a real-time basis when the document is presented.

- Has little or no biometrics, little or no electronics.

- The customer must be physically present when opening the new account.

> "*As you visualize this third scenario, how important is it that each characteristic be present on the identity document being presented? Use a scale of 1 to 5, where: 1= no importance whatsoever, or not applicable; 5=critically important.*"

Here is the fourth scenario. The identity document:

- Is legally issued only by a single centralized agency that could be either a government or private organization.

- Is issued by a process that can be trusted to ensure that the data accurately represents the applicant at the time of issue, and that the document is tamperproof.

- Data can be authenticated on a real-time basis when the document is presented.

- Contains advanced biometrics (for example, DNA, retinal scans, fingerprints)

- Contains advanced electronics (RFID chip contains electronic form of all data, and it is continuously transmitting, so that the identity document can be tracked at all times)

- Is digital, not physical

- The customer is virtual; need not be physically present when opening the new account.

> "*As you visualize this fourth scenario, how important is it that each characteristic be present on the identity document being presented? Use a scale of 1 to 5, where: 1= no importance whatsoever, or not applicable; 5=critically important*."

Finally, as you have visualized each of the four scenarios, and reviewed the list of twenty-one characteristics that seem to make identity documents more or less credible, please tell me if any other characteristics should be included. Other than the items listed, are there any attributes of the different document types that you think about when you are evaluating their credibility for opening a new account?

VITA

KENNETH ROBERT ST. LEGER HENRY

1973-1977	Price Waterhouse & Co. Kingston, Jamaica
1980	B.Sc., Computer Science University of Windsor Ontario, Canada
1980-1992	Coopers & Lybrand Miami, Florida
1992-1998	Miami-Dade County Miami, Florida
1994	M.A., Accounting Florida International University Miami, Florida
1998-2000	U.S. Department of the Treasury Riyadh, Saudi Arabia
2000-2008	Doctoral Candidate. in Business Administration Florida International University Miami, Florida

PUBLICATIONS AND PRESENTATIONS

Henry, K., Lee, R. (2007). *Document Credibility as a Heuristic for Potential Identity Fraud*, 16th Annual Research Workshop on: Artificial Intelligence and Emerging Technologies in Accounting, Auditing and Tax, Chicago, Illinois

Lee, R., Dutta, K., Henry, K., and Nguyen, V. (2007). *Controls as a Sharable Knowledge Commodity: An Architecture for Open Exchange*. Group Decision and Negotiation 16 (2): 143-167

Lee, R., Henry, K. (2006). Open *Exchange of Administrative Controls*. Formal Modeling of Electronic Commerce (FMEC) Workshop, Amsterdam, NL.

Henry, K., Clemmons, S. (2005) *Reducing Risk in the Enterprise: Proposal for a Hybrid Audit Expert System*, 7th International Conference on Enterprise Information Systems (ICEIS), Miami Beach, Florida

Henry, K. (2002) *Knowledge Assets: Governmental Measurement Standards*, Florida Artificial Intelligence research Symposium (FLAIRS), Pensacola Florida, September 2002