Journal of Forensic & Investigative Accounting
Vol. 2, Issue 3, Special Issue, 2010

Are You Really Someone Else? Determining the Credibility of Identity Documents

Kenneth R. Henry
Ronald M. Lee*

I. INTRODUCTION

Victims of personal identity theft currently number 9-10 million per year in the United States, or roughly 4% of the US adult population. The average annual fraud per stolen identity was estimated at $6,383 in 2006, up approximately 22% from $5,248 in 2003; an increase in estimated total fraud from $53.2 billion in 2003 to $56.6 billion in 2006. (Javelin, 2006)

About a third of these identity theft cases, around three million Americans each year, are 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. New account fraud is much more time consuming - and typically more costly - to repair than fraudulent use of existing accounts.

New account fraud, as well as other kinds of identity theft, depends on the bank or other organization accepting the presented identity documentation. Typically, a variety of different documents is required. A bank may decide, as a matter of its policy and procedures, that certain documents are credible evidence of a person's identity.

But 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 to estimate identity theft risk associated with the identity document types reviewed.

Our goal here is to help organizations to answer these kinds of questions - what are the characteristics that make identity documents credible? More specifically, the practical contribution is of this research is to develop a methodology to elicit critical attributes in experts' evaluation of the credibility of documentary evidence ... applied in the identity theft domain ...

* The authors are both at Florida International University.

resulting in the inter-organizational synthesis of knowledge of the critical credibility attributes elicited.

Our examination of the components of credibility draws on personal construct psychology, the underpinning for the repertory grid technique, which is 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. Our contribution is thus 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 identifies 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. Our objectives are 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.

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 theft that should be the focus in developing solutions for the identity theft problem. Having specified the attributes, how do experts rate their relative importance? Measurement of identity theft 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.

Our research goal is thus to measure credibility of identity documents, as a metric for potential identity theft. 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.

The remaining sections of this paper are organized as follows. The next section, II, describes the objectives of the research, and gives background about identity theft, including definitions, types, statutes, and regulations. Following that, section III examines various identity theft techniques, and how credibility of an identity document may be established and compromised. Next, in section IV we focus more specifically on the notion of credibility of identity documentation. Section V then describes a proposed methodology based on repertory grids, to elicit experts' knowledge about key indicators of identity document credibility.
Section VI describes the study we have done that illustrates the use of this methodology. Section VII discusses the results of this study. Section VIII has concluding remarks.

II. WHAT IS IDENTITY THEFT?

CHARACTERISTICS OF PERSONAL IDENTITY

We think of identity as those special characteristics that define who we are, what makes us special and distinct from all other human beings. However, regarding identity theft, the concerns are more mundane. Identity theft is about rights of access – to your bank accounts, to your medical insurance, to your pension benefits, to vote, to travel internationally – any of your rights as a unique individual and citizen. Identity theft occurs when someone gains illegal access to your rights. In most typical cases, another person deceives an institution, such as a bank, into believing they are you. This deception needs to succeed only long enough for the thieves to gain access to your assets and escape. Thus, identity theft is not a complete impersonation of another person in all aspects. It is only related to the individual and some institution(s). Logically, identity theft is like a thief getting a physical key to your house or safe. A closer metaphor is when a thief gets the numeric sequence to a combination safe.

Typically, the institution 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 institutional resources -- for instance, the individual may be an employee, customer, supplier, owner, or a member of a professional association. In any event, the institution 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

institution can authenticate the claimant, to be sure that the correct individual receives the correct affordances. Note that identity theft works only with impersonal institutions – that know their clients based on symbolic data. If for instance you had close relatives working at the institution, they would detect the fraud through the seeing and hearing the other person (in essence, direct biometrics).

DEFINITION OF IDENTITY THEFT

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 theft 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 theft, 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.

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." (The Federal Law Group, 2008) 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 & Foley, 2003). Here we focus only on the first of these three types. Note there 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 theft relates to 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.

KINDS OF IDENTITY THEFT

Identity theft may occur whenever there is the opportunity to impersonate another (legal) person to obtain access to assets or rights. Following is a list of the more common forms of identity theft.

Financial identity theft 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", 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). It is the recognition of this high-risk true-name fraud in opening new accounts that has caused the increasing requirements for financial institutions to “know the customer.”

Medical identity theft 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.

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).

Illegal entry is the use of identity documents to gain access to a secure facility or to cross national borders. 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, 2002). 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).

EXTENT OF IDENTITY THEFT

The largest case of identity theft in U.S. history (FBI, 2004), at least through 2004, began with a crooked "insider" who had access to a large 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.

In the United States, the number of victims of identity theft 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 theft, 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 theft: 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 theft (USDOJ, 2007), where " ... 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."

III. IDENTITY THEFT TECHNIQUES

The identity theft process is described very well in the literature, for example (Willox Jr., Gordon, Regan, Rebovich, & Gordon, 2004). We present an adaptation of their sketch of the identity theft process in Exhibit 1. This process can be divided into three major stages, which we call the A-B-Cs of identity theft:

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 using 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 theft, as none of the documents correctly represent the fraudulent applicant - the situation described as the potential for identity theft.

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.

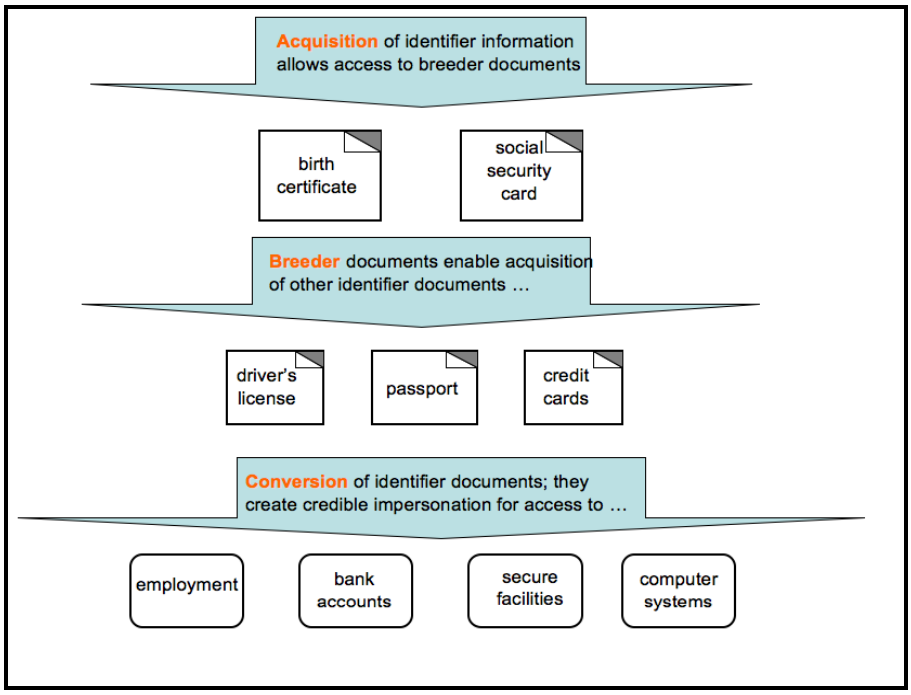

Exhibit 1. The Identity theft Process

Regardless of the environment, one important phase in the identity verification process is at the beginning. 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. & 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.

As seen in the process of committing an identity theft, it is seldom perpetrated with just a single organization. Rather, it is an inter-organizational problem. 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".

IV. DOCUMENT CREDIBILITY

This research is based on the notion that the measurement of credibility of different types of identity documents is a good metric for estimating the reliability of the identity document in preventing identity theft.

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 & 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.

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, & Kelley, 1953; Hovland & 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 & Nass, 1989; Quinn, 2004; Slater & 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, 1994; Bateman, 1998; Cool, Belkin, & Kantor, 1993; Schamber & Bateman, 1996; Wang & Domas-White, 1999) with researchers focusing on how information seekers assess a document's likely level of quality (Liu, 2004; Rieh, 2002).

A WORKING DEFINITION OF CREDIBILITY

This research targets the credibility of 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 & 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 & 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.

Credibility assessment involves 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.

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.

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.

DETERMINING CREDIBILITY OF IDENTITY EVIDENCE

What procedure should a bank adopt in verifying the identity of a new potential customer? Of a returning customer? For banks, controlling for identity theft is a trade-off. On the one hand, they need to take measures to insure that their clients' deposits are not stolen. On the other hand, onerous identity controls may offend potential clients. 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 non-fraudulent identity -- will result in lost revenues as potentially profitable new customers are turned away. We would like to help banks and other financial organizations determine which kinds of documents to rely on in their identity verification procedures.

There is no fixed answer to this question - it depends on a bank’s specialization, geographical location, and the profiles of its customers. However, banks have access to various experts that have long experience in fraud detection. We now describe our proposed method for eliciting the criteria that experts use in deciding the credibility of identity evidence, and to pool their collective wisdom.

V. METHODOLOGY

This methodology borrows from a number of different, but well-established theoretical backgrounds. First, identification of the components of credibility draws upon personal construct psychology (Kelly, 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 & 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, & 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 & Nakamura, 1993; Fisher, 1922; Vogt & Barta, 1997).

REPERTORY GRID TECHNIQUE

Historically, 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, each of these methods is open to experimenter bias and subjectivity; a more neutral approach is desirable. Such an approach is provided by the repertory grid methodology. A principle advantage is to reduce or eliminate the effect of experimenter bias. We adopt the repertory grid technique for this research to help overcome the subjectivity and bias that has hindered prior research related to credibility.

Sources of bias in traditional techniques include the following considerations. 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.

Although the repertory grid technique 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.

SELECTING ELEMENTS: KINDS OF IDENTITY DOCUMENTS

In the Repertory Grid technique, elements should be selected to 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?" 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 set of twelve elements used in the repertory grid interviews. These elements are listed in Exhibit 2. 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

Exhibit 2. Identity Documents Used as Elements in Repertory Grid Interviews.

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 fraud 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.

CONSTRUCT ELICITATION

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 might 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.

From these responses, we can produce the following construct dimensions:

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. (Details of the script used to introduce each interview is included is found in (Henry, 2008) - Appendix A.

SCENARIO CREATION

A challenge for the research is that experts' judgment would be expected to change with time and environment. We accommodate these different contexts by introducing a notion of scenarios. We 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). For example, some of the shifts in perceptions in the area 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.

There are various guidelines for the construction of scenarios. For example, (Schoemaker, 1993) proposes a ten-step method. Six trends were identified from the interviews, as listed in Exhibit 3. Using the Schoemaker's ten steps, we created four scenarios by grouping the six trends into two sets of three as shown in the two-by-two matrix in Exhibit 4. Scenario #1 was contrived to be the closest to a current situation, and #4 as the most futuristic, without being unrealistic. The features of the scenarios are summarized in Exhibit 5.

A. 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.

Exhibit 3. Six Trends for Identification Procedures

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)

Exhibit 4. Trends and Scenarios for Identity Document Evaluation

SCENARIO #1.
- 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.

SCENARIO #2.
- 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.

SCENARIO #3.
- 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.

SCENARIO #4.
- 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.

Exhibit 5. Scenario Features

VI. STUDY DESIGN

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. The 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). The survey focused only on financial identity theft. 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.

Only the construct elicitation phase of the repertory grid method was 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.

During the process of eliciting the characteristics of credibility from the experts, they were 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. 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. These trends were 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.

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 (Henry, 2008, Appendix 2). 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.

VII. SUMMARY OF RESULTS

As explained earlier, four different scenarios were used in the interviews. The study results included a repertory grid 'focus' graphic for each of the scenarios, together with an analysis of the information conveyed. To illustrate, Exhibit 6 shows the results for Scenario #1. 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. Continuing with Exhibit 6, the 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 exhibit, 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.

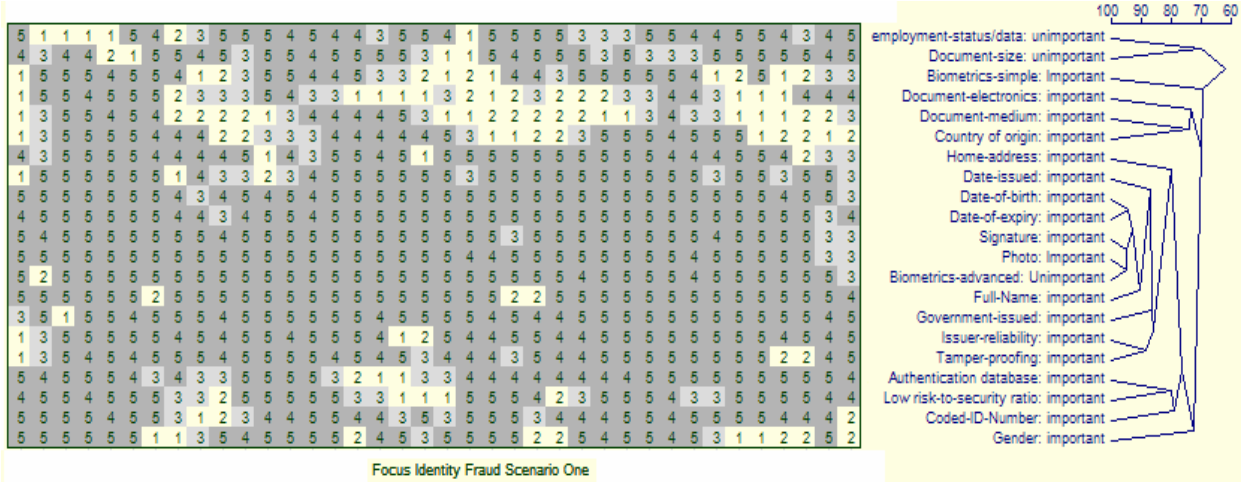

Exhibit 6. Repertory Grid Focus Scenario #1

A synthesis of the highest consensus results across all scenarios is shown in Exhibit 7. The strongest consensus was 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. By contrast, 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.

These results suggest a need for further research to explore this apparent expectation gap. 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 theft 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.

	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

Exhibit 7. Synthesis of Results

VIII. CONCLUDING REMARKS

The main focus of this research has been 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 theft research, as it provides a qualitative answer to the question, based on knowledge acquired from experts in a variety of financial service 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 theft 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 resulted from these interviews, as listed in Exhibit 8. These are the attributes of identity documents that affect the evaluation of a

document's credibility for banking experts reviewing them as part of the new account opening process. Most are self-explanatory; the few exceptions include some brief discussion

The six trends identified during the first round of interviews represent another contribution to the practice of identity theft 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. These trends were summarized in Exhibit 3.

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 high risk exposure associated with successfully presenting a fraudulent identity document, while at the same time, security features on the document are at a relatively low level, resulting in a high risk to security ratio.
20. Signature
21. Tamper-proofing (laminates, seals, holograms)

Exhibit 8. Document Features Affecting Credibility Evaluations

CONTRIBUTIONS

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 theft. That should be the focus in developing solutions for the identity theft 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 theft 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 instance, biometric data is considered to be one of the most secure forms 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. US border inspectors have a hard time detecting passports known as 'stolen blanks' -- 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 same 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" (Dateline-NBC, 2007).

LIMITATIONS

Our main purpose here is to propose an application of the repertory grid technique as a means to elicit the criteria that experts use to assess the credibility of identity documents. We have illustrated the use of this technique by a pilot study. While the results of this pilot study have been useful and informative, it has limitations due to its relatively small size and limited geographical scope. However, the limitations due to small sample size are 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.

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 & 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-to-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.

EXTENDING THE STUDY

The pilot study could be extended in various ways. For example, the 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. 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.

As previously noted, the current study used only the construct elicitation phase of the repertory grid method, recognizing the practical constraint that 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 example, of a principal components analysis of credibility in identity documents.

REFERENCES

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

Barry, C. L. (1994). User-Defined Relevance Criteria: An Exploratory Study. *Journal of the American Society for Information Science, 45*(3), 149-159.

Bateman, J. A. (1998). *Modeling changes in end-user relevance criteria : an information seeking study*. Unpublished Dissertation, University of North Texas, Denton, TX.

Burbules, N. C. (2001). Paradoxes of the web: the ethical dimensions of credibility. *Library Trends, 49*(3), 441-453.

Collins, J. M. (2003). Business Identity Theft. *Journal of Forensic Accounting, 4*(2), 303-306.

Cool, C., Belkin, N. J., & Kantor, P. B. (1993). *Characteristics of texts affecting relevance judgments*. Paper presented at the Proceedings of the 14th National Online Meeting.

Dateline-NBC (Writer) (2007). Passport investigation suggests security hole. USA.

Diewert, W. E., & Nakamura, A. (Eds.). (1993). *Essays in index number theory* (Vol. 1). Amsterdam, The Netherlands: Elsevier Science Publishers.

Dixon, P. (2006, May 3). Medical Identity Theft: The Information Crime that Can Kill You. *World Privacy Forum* Retrieved June 24, 2007, from http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf

FBI. (2004, October 18). No Ordinary Case Of Identity Theft. Retrieved July 15, 2006, from http://www.fbi.gov/page2/oct04/uncoveridt101504.htm

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

Foley, L., & Foley, J. (2003). Identity Theft: The Aftermath 2003. *Identity Theft Resource Center* Retrieved June 3, 2007, from http://www.idtheftcenter.org/artman2/uploads/1/The_Aftermath_2003.pdf

Fransella, F., & Bannister, D. (1977). *A Manual for Repertory Grid Technique* (1st ed.). New York, New York: Academic Press.

GAO. (2002). *Identity Fraud: Prevalence and Links to Alien Illegal Activities*. Retrieved. from http://www.gao.gov/new.items/d02830t.pdf.

GAO. (2005). *Improvements Needed to Strengthen US Passport Fraud Detection Efforts*. Retrieved. from http://www.gao.gov/new.items/d05853t.pdf.

Henry, K. R. (2008). *Attributes of Identity Document Credibility: A Synthesis of Expert Knowledge*. Unpublished Dissertation, Florida International University, Miami, Florida.

Heyer, R. (2004). *Understanding Soft Operations Research: The Methods, Their Application and Its Future in the Defence Setting*. Retrieved August 18, 2007. from http://www.dsto.defence.gov.au/publications/3451/DSTO-GD-0411.pdf.

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

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

Hovland, C. I., & Weiss, W. (1951). The Influence of Source Credibility on Communication Effectiveness. *The Public Opinion Quarterly, 15*(4), 635-650.

Howard, H. M. (2005). The Negligent Enablement Of Imposter Fraud: A Common–Sense Common Law Claim. *DUKE LAW JOURNAL, 54*(5), 1266.

Identity Theft and Assumption Deterrence Act (1998).

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

Javelin. (2006). New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think. *Javelin Strategy and Research* Retrieved July 7, 2006, from http://www.bbb.org/Alerts/article.asp?ID=651

Kelly, G. (1955). *The psychology of personal constructs I and I.I*: New York: WW Norton.

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

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

Liu, Z. (2004). Perceptions of credibility of scholarly information on the web. *Information Processing and Management: an International Journal, 40*(6), 1027-1038.

Meyer, P. (1988). Defining and measuring credibility of newspapers: Developing an index. *Journalism Quarterly, 65*(3), 567-574.

Nass, C., & Mason, L. (1990). On the study of technology and task: A variable-based approach. In J. Fulk & C. Steinfeld (Eds.), *Organizations and communication technology* (pp. 46-67). Newbury Park, CA: Sage.

Newhagen, J., & Nass, C. (1989). Differential criteria for evaluating credibility of newspapers and TV news. *Journalism Quarterly, 66*(2), 277-284.

Quinn, J. V. (2004). *A measurement of credibility in the forensics realm.* Unpublished M.A., California State University, Fullerton, United States -- California.

Reeves, B., & Nass, C. (1996). *The media equation: how people treat computers, television, and new media like real people and places*. New York, NY: Cambridge University Press

Rieh, S. Y. (2002). Judgment of information quality and cognitive authority in the Web. *Journal of the American Society for Information Science and Technology, 53*(2), 145-161.

Rieh, S. Y., & Belkin, N. J. (1998). *Understanding judgment of information quality and cognitive authority in the WWW.* Paper presented at the Proceedings of the ASIS Annual Meeting.

Roberts, F. S. (1979). Measurement Theory, with Applications to Decisionmaking, Utility, and the Social Sciences. In G.-C. Rota (Ed.), *Encyclopedia of Mathematics and its Applications* (Vol. 7). Reading, Massachusetts: Addison-Wesley Publishing Company.

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

Schamber, L., & Bateman, J. (1996, October). *User criteria in relevance evaluation: Toward development of a measurement scale.* Paper presented at the Proceedings of the American Society for Information Science, Baltimore, MD.

Schoemaker, P. J. H. (1993). Multiple Scenario Development: Its Conceptual and Behavioral Foundation. *Strategic Management Journal, 14*(3), 193-213.

Slater, M. D., & Rouner, D. (1996). How message evaluation and source attributes may influence credibility assessment and belief change. *Journalism and Mass Communication Quarterly, 73*(4), 974-991.

The Federal Law Group. (2008). Trends in Corporate Liability. Retrieved June 7, 2010, from http://www.federallawgroup.com/CM/Custom/Corporate-Crimes-Trends-Corporate-Liability.asp

Towle, H. K. (2004). Identity Theft: Myths, Methods, and New Law. *RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL, 30*(2), 242.

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

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

Wang, P., & Domas-White, M. (1999). 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*(2), 98-114.

Willox Jr., N. A., Gordon, G. R., Regan, T. M., Rebovich, D. J., & Gordon, J. B. (2004). Identity Fraud: A Critical National and Global Threat. *Journal of Economic Crime Management, 2*(1).

Willox Jr., N. A., & Regan Esq., T. M. (2001). Identity Fraud: Searching For A Solution [Electronic Version]. *White Paper*. Retrieved July 16, 2006 from http://www.lexisnexis.com/risksolutions/IdentityFraud.pdf.

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