# Submission for CFP 2004

# Student Competition

# Security Document Theory Whitepaper

By James Moyer

james@moyer.com

*James Moyer is an undergraduate at the Ohio State University, majoring in Economics and Russian Linguistics. Since 1998 he has been involved in data privacy and ID card issues; starting the Buckeye Privacy Coalition, a student group devoted to changing Ohio State's privacy and data retention policies, successfully lobbying the Ohio legislature for pro-privacy legislation, assisting the driver's license privacy fight in Texas, and, with his new NJlicense.org project, fighting to keep the non-photo driver's license in New Jersey.*

*In the summer of 2003 he wrote the Security Document Theory whitepaper, an attempt to explain the framework of photo ID card security. The current version of SDT is always available at http://www.njlicense.org. SDT is hereby submitted for consideration in the CFP 2004 student paper competition.*

# Security Document Theory White Paper

## Summary

Fraud is implicit in society. Often, solutions, like photo ID cards, create more potential for fraud than the fraud they eliminate. Security Document theory explains how. As long as a document can be used for fraud, the cost to counterfeit it will likely be less than the value to the criminal. Documents, which allow an individual to perform multiple fraud-tasks, are even more valuable. When people perceive the document as implying trust in a security situation then the document becomes a weak point in the safety of society.

## Definitions

Documents that are used to prove evidence of something are security documents. Money is a security document of wealth/value, college transcripts are security documents of course work accomplished and photo ID cards are security documents of identity[1] veracity (as are birth certificates, Social Security Cards, et cetera.) Security documents have **security values**, the probability that the document is genuine and conveys the correct information for the situation. A **misrepresenting document** is a document that conveys the wrong information about an individual, but is accepted anyway. A **faked** or **counterfeited** security document is one that has been carefully made by a fraudster to look like a genuine document; the complexity of making the document is measured by the **counterfeit difficulty value**. Compare this to a **fraudulent** document, one which is genuine, in that it was obtained from a legitimate source, but does not

[1] "Identity" can often refer to two different concepts. One is where the individual is the only one to be identified, and their name or their ID number is correlated to them personally (if this were done with a photo ID card it would be done in a **name-and-face transaction**.) The other is to see if the individual belongs to a particular class of individuals (like those over the age of 21, or who are citizens of country X) but their own personal name is irrelevant (**class-membership transaction**.) The latter is much more common, and rarely are both name-and-face and class membership verification done at the same time. Furthermore, there are **tracking transactions** in which the photo ID card may be used not to actually identify the individual as much as to make a way to find them should it be necessary. A photo ID card used to write a check is an example…the identity is irrelevant, but may become relevant if the check fails. Security transactions, which do not fall into either of these categories, are **psychological confidence failure transactions.** (The word failure appears because a bad ID card may allow a person to do something they wouldn't have been able to do without the ID check in the first place.)

convey the correct information (for instance, a photo driver's license obtained through the bribing of a DMV official would be a fraudulent document.) Interplaying with the security value is the **trust value**, which is what humans perceive as the security value of the document. In comparison to the security value, the trust value is entirely based on how humans perceive a particular document. Related to trust value, the **psychological confidence factor** is a human deficiency that causes individuals to overrely on some types of security documents and glean information from them that the document does not imply ("social engineering."[2]). Finally, the **misrepresenting value** is the value to fraudsters of obtaining a fake or fraudulent document. A non-photo New Jersey license, while easy to counterfeit (low counterfeit difficulty value) is rarely counterfeited, because it's misrepresenting value is low. On the other hand, a California photo license (high counterfeit difficulty value) is often counterfeited since it can be used in many nefarious ways.

There are five different ways an individual can obtain a security document to misrepresent themselves:

- Counterfeiting the document
- Altering the document (to read different, to a human and/or a machine)
- Using someone else’s legitimate document
- Misrepresenting using other security documents (such as a birth certificate or Social Security Card, either someone else’s or counterfeit) to an issuing official to obtain a fraudulent document
- Using bribery or internal connections with issuing officials to obtain a fraudulent document

This list is important because attempts to reduce security document fraud are most effective if they control all of those factors. Each of those routes will have some type of expense involved (**misrepresenting cost** takes all the misrepresentation routes into account), so if only one or two of the ways become difficult, then another way will be more appealing. The hazard to this is that controlling one factor is not without side-effect. Making a photo license document more difficult to counterfeit will raise trust values, but may not change other misappropriation strategies, erasing any gains made.

## Security Value

The security value is the most understood component to the security document equation. The security value is essentially the probability that the card is valid and that the information is good for the situation at hand. Clearly this value changes with what kind of card it is, the situation in which it is being accepted, who the issuer is, the structure of the card, et cetera. *The most important factors affecting the security value are the number of cardholders and the misrepresenting value of the card*. The security value of the photo driver's license in the situation of a police officer pulling a motorist over is high; people do not fake driver's licenses to drive automobiles; while fraudulently issued cards are possible, individuals who cannot get licenses for one reason or another usually drive taking the chance that they will not be pulled over. This is one reason why non-photo licenses work so well for driving (the physical description of the person prevents the card from being taken by another random individual and used, while the lack of the

[2] Computer security experts know that the biggest weakness in a network security situation is the human factor. The biggest computer hacking moments occurred not because of brilliant computer “hacking” but because of a person obtained a password by pretending to have a legitimate use for it. The process of manipulating humans to get past security regimes is called social engineering.

photograph prevents the card from being used in situations unrelated to driving, where a higher trust value is required.) Compare this to photo licenses being used in a bar, where the security value of the license is significantly lower because underaged individuals have a strong interest in having authentic looking documents to drink, and in pursuing that, lowers the security value of all the documents shown in that bar. (Interestingly, barmen spend quite some time examining the photograph of the individual and the authenticity of the document, while ignoring the physical description. Often, individuals will use authentic photo ID cards of older friends, who look approximately like them, but do not share their physical dimensions/eye color. It appears that humans try to "squeeze to fit" the facial features of the photograph on the card into the facial features of the individual presenting the card. We have a much more powerful ability to morph faces in our minds than we realize, which is odd since we put so much faith in photograph based documents. For this reason, photographs artificially increase the trust value of photo ID documents.)

## Trust Value

The trust value is the least obvious component of security document theory. Recall that the trust value is simply the human perception of the security value of the document. Often, for many different reasons, individuals overtrust documents, so that the trust exceeds the security value of the document. An interesting example of this is aesthetics on driver's licenses: some states produce more colorful, attractive license documents. The human eye may be entranced by the aesthetics, and, in comparison to a less attractive document, an individual may assume that the nicer looking document is harder to counterfeit. In reality, the two documents may have the same counterfeit difficulty value, but the aesthetics of one will evoke a higher trust value. A fraudster would therefore be wise to counterfeit the aesthetically attractive document, as it is more likely to be accepted.

Consider another example of state standing. Because of the ubiquity of the California driver's license, its easy to recognize design, and other factors, it has a high trust value; and likely a higher trust value than a much harder to find document, such as a Wyoming driver's license. This is a tremendous error, Wyoming issues a significantly smaller amount of driver's licenses from far fewer DMV offices; the probability that any one Wyoming license is fraudulent is far lower than that of a California license. However, we are much more likely to trust the California license, even if it has the lower security value. Recall that the number of cards affects the security value. Wyoming, based on its population, likely issues no more than 300 cards per day, whereas California issues 25,000 per day, and fraudulent ID issuance rises dramatically with the number of cards issued. Because California has seventy times more people, it may be assumed that California has 70 times more counterfeiters than Wyoming.

Essentially the trust value of the card is poorly correlated with the security value, especially when the trust value is increased by ubiquity, and the same decreases the security value. Eventually the trust value of a security document will collapse in a **trust failure** (and anytime 2 forms of ID are required you’ve had a trust failure. Examples of this include some state DMVs no longer accepting birth certificates as identification documents, or some restaurants/bars requiring 2 ID documents for alcohol purchases.

Outside of North America, trust failures are common with national identification cards (law enforcement in those countries may not believe the authenticity of the card, and require the citizen to be identified through other means.) A variation of this theme is happening in Virginia, where individuals who have been mistaken for other individuals, or been victims of identity fraud, can apply for an “identity theft passport”—a document indicating to law enforcement that they are (most likely) not the one the police are seeking. Essentially, they need more documents to support the veracity of their current photo ID document.

## Psychological confidence—effects on security situations

An unknown individual is coming to your door. This individual has a laminated photo ID card around their neck. Because of this, it is likely that you will be given confidence in opening the door and will be more at ease.

This is entirely unwarranted response—simply caused by a plastic card. However, photo ID cards do have some type of psychological effect that causes humans to overtrust unknown individuals (the fact is, even with a photo ID card, they still remain unknown.) The effects of this are disastrous with regards to identity (in that fraudsters can leverage the psychological confidence weakness in ways that would not have been possible with non-photo documents.) The effects in security conscious situations are more severe…photo ID cards offer the terrorist all new weak points for exploitation, because the documents themselves evoke too much confidence and trust. Naturally the psychological confidence factor directly raises trust and misrepresenting values.

## Misrepresenting value

The misrepresenting value is determined by the trust value, and the real world uses of the security document.[3] The $1 bill has a low misrepresenting value; the resources required to counterfeit a $1 bill simply don't justify counterfeiting because a fraudster spend more counterfeiting the bill than $1. The $100 bill has a very different misrepresenting value; while it is not much harder to counterfeit than the $1 bill, a fraudster's investment into it may very well pay off. (On the other hand, it's arguable that the $100 has undergone a trust failure, in that many merchants refuse to accept it. A good fraudster would be well advised to figure out how to counterfeit large quantities of smaller bills, which have a higher trust value.) It should be added that the misrepresenting value of currency drops with time due to inflation. This, in addition to new currency design, means that counterfeiting of small bills decreases with time. [4]

## Document structure and manufacture

Sometimes a currency note is altered to be a note of higher value, instead of being counterfeited from scratch. This happens with photo ID documents as well. In these days of plastic license cards protected by a variety of tamper-resistant devices, the weakness is not the

[3] This is important because as trust value for a document increases, institutions will be more willing to accept the document for more uses, thereby increasing the misrepresenting value. Sometimes, this happens just with time; consider how institutions used photo driver's licenses within the first ten years of their appearance, in comparison to how they are used now. Institutional usage of photo ID cards also increases dramatically if individuals are assumed to have one, such as in a state like California, with a high percentage of licensed drivers, in comparison to a state like New Jersey, with a lower percentage of licensed drivers, some of whom have non-photo licenses. Institutional expectation and usage of photo ID cards are the components that make the **photo ID culture**. The photo ID culture (factor) directly affects misrepresenting values, which aren't so much components of the security document equation, as much as a result.

[4] Keep in mind that while currency is always dropping slightly in misrepresenting value, the current photo ID culture in North America is causing photo ID cards to increase in misrepresenting value. On exception to this is the passport, which can be used for name-and-face transactions, but is really just used for class-membership transactions (individual is citizen of country X.) A smaller type passport document that would be card-like would dramatically increase passport fraud, since it then would be usable in other situations, and thereby have a higher misrepresenting value. The State of Georgia has plans to print an individual's country of citizenship on their driver's licenses, a decision that can only extend the uses of the document, causing a higher misrepresenting value, and therefore more fraud.

text on the documents, but their machine-readable elements. In spite of everything, a counterfeit document has to be of quality in some way to fool a human[5] but all a machine needs to see is a magnetic stripe or barcode, which has the correct combination of bits and lines. It is significantly easier to alter a document so that it reads differently by a machine (remagnetizing the magnetic stripe, redesigning/relabelling the barcode, et cetera.) The experience with humans and machines is thus: a human will quickly glance at a photo ID presented, only to ensure that the picture more or less resembles the presenter, and then swipe the card through the machine which takes care of the rest. (If the human had to also ensure the integrity of the card and check the data printed on it, then the machine is clearly unnecessary. If the purpose of the machine is not to check the data (like confirm that the individual is over 21) but to confirm that the card was issued by a trusted agency, then a counterfeiter with the means to counterfeit the card well could clearly counterfeit the machine readable elements as well.) Therefore, machine-readable elements open a new door of weakness for security documents and are highly advised against.

## Security Document Theory Applied

In order to evaluate a change to a security document framework, run the proposal through a Security Document Theory matrix to see the results.

- ✓ **Which misrepresentation strategies are affected?**
- ✓ **How is trust value affected?**
- ✓ **How is misrepresenting value affected?**

**What is Security Document Theory's evaluation of New Jersey's proposal to change to a digitized driver's license?**

**Misrepresentation strategies**

| | |
|---|---|
| Counterfeit difficulty | Will increase with more difficult to counterfeit document |
| Alteration difficulty | More difficult to alter for human readability, easier to alter with new machine readability elements |
| Using someone else's document | No change |
| Misrepresenting using other security documents | Essentially unchanged—proposals are in place to require a "six-point identity verification" which increases the quantity of documents required for proof of identification. However, most of these documents are unremarkable and easy to counterfeit |
| Bribery/internal connections | No change |
| **Trust Value** | New document inspires significantly higher trust and confidence |

[5] There are many counterfeit strategies. If an individual needs to counterfeit a state ID card, but doesn't have to do their own state's card, they would be advised to do an out-of-state card. An individual in Ohio knows the Ohio license well and may be able to spot defects in it, but would have difficulty spotting defects in an Ontario license, even if they have a schematic of said license.

| | |
|---|---|
| **Misrepresenting value** | Significantly higher trust value creates new fraud opportunities with new document, thereby increasing the misrepresenting value |
| **Conclusion** | **Unless misrepresenting value is somehow controlled (perhaps through trust value) more document fraud is inevitable; the misrepresentation strategies that have changed are likely overwhelmed by the higher misrepresenting value** |