After obtaining a SSN and an associated address, the attacker obtains credit. Initially, the attacker pays only the minimum due. Such a practice provides the highest possible credit rating.

Identity theft is the major common individual risk because of identity-based systems. The efficacy of identity theft is based on the fragility of the SSN-based identity system. Social Security Numbers enable federated identity systems. Because of the federation of multiple identities, one authenticating element can be used to generate reams of credentials.

No one has one key for their entire lives – one that opens the car, the safety deposit box, the house, and the desk. Different keys are controlled by different entities. The bank issued the safety deposit box key; and an employer issues the key for the building. Yet each of these places shares one key in the digital databases when ownership information is stored – the Social Security Number.

A SSN is required to obtain and sign a mortgage, or for a credit check to rent. A SSN is required to open a bank account and obtain a safety deposit box. An SSN is required as identification to get a job. A SSN is officially not required to obtain phone service; however, phone companies often simply refuse by not responding to requests with other identification. Having one key shared by all these organizations for all the locks in a person's life is unwise in terms of security and risk management, a disaster waiting to happen. It is this consistent relentless practice in the information realm that has caused identity theft.

Who would design a system where one key fits every lock in a person's life, and that person is required to give copies of the key to everyone with whom they have any chance of sharing a lock? It is tempting to explain this away with some false wisdom, like the jokes about committees where "None of us is as stupid as all of us." But in fact it is something more fundamental than the tendency of bureaucracy to use what works until it fails catastrophically. The one-lock-fits-all is based in part of the agrarian concept of identity that is deeply embedded in our humanity; that is, the idea that we have a single meaningful social and human identity.

Most importantly, the design is a result of *failure to design*. One system worked. Reliance on that system resulted in a collective failure to effectively move authentication and identifiers into the information age. The credit agencies and data brokers that profit dominate the resulting policy debate.

Paper-based identity systems link attribute, identity, and authentication into a single stand-alone document. SSNs worked fairly well in a paper-based system. The availability of networked data opens entire new vistas of possible systems. However, it simultaneously destroys the assumptions on which paper-based systems are built. Networked data is undermining the assumptions of "secret" information on which paper systems depend. "Secret" information is not information that is in every database, from Amnesty International donation records to the Zoo Family Membership.

The risks created by this shift are not equally distributed. Organizations can utilize the value of databases without protecting them. The value to the organization is in having the data; not in preventing others from having what is essentially public data.

Identity theft victims for a very long time were quite left in the cold. However, now that identity theft is the fastest growing crime, victims have some company and some legal support. There is Federal legislation making identity theft a crime. Before that legislation it was sometimes difficult to obtain a police report, as needed in recovery for identity fraud.

The Identity Theft Assumption and Deterrence Act, (918 USC 1028) in addition to prohibiting the construction of fake identification documents regardless of their use, requires the Federal Trade Commission record these complaints. However, the FTC does not investigate the complaints, rather the FTC keeps a database of cases, uses this database for research and tracking of cases, and provides a listing of law enforcement agencies that investigate complaints. The complaint numbers from identity theft victims obtained under the law must be provided to Federal officials in order to track the problem as it expands. Currently the FTC has a database approaching a million identity theft cases.

The Fair and Accurate Credit Transaction Act of 2003 defined identity theft as “fraud, attempted or committed using identifying information without authority”. The FACT enabled ID theft victims to place 'fraud alerts' on credit files, and thus decrease the risk of loss in the future. FACT also created a National Fraud Alert system.

The 2004 Act greatly increased penalties for identity theft, however, the practices that lead to identity theft (in particular the use of Social Security Numbers by businesses) have not been curtailed. Interestingly enough, the 2004 bill included particularly stringent punishments for using identity theft in conjunction with a terrorist attack. This explicit recognition of the use of identity in implement terror attacks is almost as explicitly ignored in anti-terror programs, as some proposals function only if identity theft were not possible.

State laws that cover identity theft also usually cover criminal identity theft. Yet some are too focused on identity theft as a financial act, rather than as a device to commit other crimes. For example, the Massachusetts law makes it criminal to obtain information in order to pose (“falsely represent oneself, directly or indirectly, as another person”) as another person or to obtain financial gain or additional identity information.

Specific identity theft laws have been passed in the majority of states, more than forty. In the remaining states identity theft is covered under fraud statutes and prohibitions on providing false information in a police report. Yet no state has a comprehensive mechanism for recovering from criminal identity theft. Once a criminal assumes a trustworthy identity as an alias, that identity cannot be trusted.