Identity Theft and U.S. Data Protection Legislation

Identity theft and identity fraud have been growing in epidemic proportions all over the world.

WinEncrypt

Identity Theft and U.S. Data Protection Legislation

Identity theft and identity fraud have been growing in epidemic proportions all over the world. Identity theft is generally used for instances where a person wrongfully acquires personal information about another individual and uses this information for economic gain. Popularly known as iJacking, breach of privacy has become a serious problem, 86,000 Americans complaining of their personal information being used by others in 2001. This figure rose to around 9.9 million people who complained of identity theft in 2007, with the total was estimated loss for consumers estimated at approximately $5 billion.

How is personal information stolen?

Personal information under Sections 1798.80-81 contains only name, phone number or residence address. Personal information can often also include credit card numbers, bank account numbers, passwords, etc. There are a number of routes through which data theft is perpetrated:

- ✓ Emails containing personal information
- ✓ Shoulder surfing at ATMs or Internet cafes
- ✓ Advertisements for job offers that are actually fake to track personal data of candidates
- ✓ Pretending to be a representative of a well known organization, for example a bank or government institution
- ✓ Software hacking for passwords, credit card information etc.

U.S. Laws Pertaining to Personal Data Protection

Although there aren't any comprehensive laws in the United States regarding the notification of theft of personal data, some specific laws have been enacted pertaining to identity theft.

The Identity Theft and Assumption Deterrence Act was enacted in 1998 by the Congress to keep data theft under control. According to this law, nobody can knowingly use personal information of others with the intention of committing any illegal activity that might call for a legal action. Anybody caught violating this Federal law will be liable to rigorous imprisonment of 15 years in a federal prison. The Federal Trade Commission (FTC) also has also been focused on resolving the issue of identity frauds related to services, loans, mortgage, credit card, etc. The FTC has been granted authority under the Identity Theft and Assumption Deterrence Act to keep track of reported incidents of personal data theft and their monetary value. Penalties that are levied on thieves differ from state to state, depending on the gravity of the offence.

The Identity Theft and Assumption Deterrence Act received full support from the private and public sector, including the FBI, Department of Justice, United States Postal Inspectors, etc.

The state of California passed **SB 1386** legislation in 2002 for victims of identity theft, while introducing steps to be taken to protect personal information. In most of US states, data protection laws have been enforced although legislations differ depending upon the type of data and many other legal factors.

WinEncrypt™

Ways to Protect Data

Most of the cases of identity theft have been found in rich cities such as Denver, San Francisco, Las Vegas, Salt Lake City, etc. The government has issued various notices regarding data protection, such as:

- ✓ The best way to protect personal data is to encrypt it in such a manner that it becomes unreadable for unauthorized users.
- ✓ Credit card reports of consumers should be reviewed every year.
- ✓ Documents containing personal information should be destroyed at the earliest if they are of no use.
- ✓ Local law enforcement agencies should be immediately notified regarding identity theft.
- ✓ Passwords and social security numbers should be committed to memory.
- ✓ Ensure privacy at ATMs and don't forget to take your transaction receipts.
- ✓ Disclose personal information only on websites providing proper security for transactions.
- ✓ Keep a check on your bills as well as financial statements every month.
- ✓ Companies should maintain network security to save personal data of employees from being hacked.

Presence of mind is essential in cases of identity theft or identity fraud. Your funds can disappear rather quickly, following an identity theft and it is important to act immediately in order to soften the blow.

CryptArchiver: Protects files on PCs & USB Drives

- Keep your important files away from prying eyes.
- Create virtual "Encrypted Drives" upto 20 GB in size.
- Uses strong 448-bit Blowfish and 256-bit AES encryption.
- Easy to use, just drag-and-drop!
- Password-protects all types of files and folders.

Read more about free encryption software at WinEncrypt.com