Session No. 658

Identity Theft: Actions for Detection, Prevention, Redemption

Chris M. Wright, CPP
President
The Wright Group, Incorporated
Anaheim, California

Privacy Issues Apply to All

Privacy Issues will be defined in relation to individuals as well in American Business. The loss of control of privacy will be discussed as well as how the information is collected and by whom. Privacy matters will be related to identity theft. There will be proven methods on how to take offensive action before this crime is committed. Once identity is stolen, there are numerous steps that need to be taken to help with the situation as well as where to go to seek advice and counsel.

Why Identity Theft and for What Reasons?
Numerous reasons are shared on why identity theft is at its all time high. There are ways in which all firms, agencies or individuals may take action in order to prevent the crime from taking place. Information on how thieves obtain the private information and how it is used is shared with the attendees as well as questions from the audience.

Your Rights as a Victim
The victim's rights, options and guarantees will explained in relation to the following acts:

- Identity Theft Deterrence Act
- Fair Credit Report Act (FCRA)

It will be explained in a step by step basis on who to notify that you are a victim of identity theft by contacting the credit bureaus, alerting creditors in writing, reporting the crime to the police and/or the Secret Service.

What to do
There are a number of steps that must be taken in order to regain control of the victim's name and money.

- Write a description of the situation
- Re-assert control of the your bank accounts

- DO NOT pay fraudulent bills
- Get a new ATM card
- Straighten out the mail
- Alert public utilities
- Contact the Secret Service
- Notify Social Security
- Check passports
- Protect phone card/s
- Change of Driver's License Number
- Contact the auto insurer, if needed
- Clear the name used in the courts
- Consider obtaining legal assistance
- Take care of yourself
- Seek change in legislation
- Never give up. . Never quit. .Never let it happen again!

Take personal precautions by properly discarding and storing personal information. Agency, company and personal information must be guarded in public places. Pay special attention in dealing with credit cards. Protect all written and black checks. Don't give out any personal information over the phone, whether it be a land line or a cellular phone. Protect mail by obtaining a post office box or a locking residential mailbox. Opt out of mass mailings and request direct deposit to your bank accounts whenever possible. Order credit reports for all three major credit reporting agencies at least two times a year and correct all mistakes on the credits reports immediately. Block your name from marketing lists and opt out of all pre-approved credit offers.

Internet protection is a major key in prevention. Many steps may be taken to insure privacy.

- Install Firewall software.
- Inform the internet provider that personal information is not for sale.
- Do not register when visiting websites unless there are strict privacy policies.
- Do not list your company or personal name on internet online directories.
- Do not display personal or family info on line.
- Never share passwords with anyone.
- Do not trust people you meet on line,
- Teach and practice all of the rules regarding the internet with your family,

Protection in the Workplace

Each agency or company MUST have strict audit procedures and periodic check-review policies in place. The human resource departments must complete a criminal and civil background check prior to hiring new employees. This includes part time employees as well. All personal information should be kept in locked cabinets. There should be a limit on the use of personal identifiers. All confidential and personal information that is kept on computers should be encrypted. All business cards should have employee photos for identification purposes. All companies should have a proven method of dispensing of personal information. All designated staff should be trained in security procedures in sending sensitive personal information via fax. No sensitive information should be left on voice mail, cell phones, answering machines, email,

etc. at any time. Only designated, secure printers and copiers should be used for confidential information. There should be a written privacy protection policy that covers all persons within the organization and applies to dealings with persons outside the organization.

Summary

By realizing that we all have zero privacy we must all move forward to protect ourselves and our families from identity theft. In the United States, identity is established by:

- Name
- Date of Birth (DOB)
- Social Security Number (SSN)

After following the outlined steps for prevention at home, on line and the workplace more people will be educated on how to secure their privacy. If some have discovered that their identity has been stolen then the discussion on how to begin the process on how to regain possession of one's own identity should be followed through, step by step, in accordance with the process. It is a tedious task and a bit of a process but one should NEVER give up, NEVER quit and above all NEVER let it happen again.