HILL & USHER
Insurance. Bonds. Benefits.

Identity Theft 2.0

Sunday, August 16, 2011

PHOENIX (H&U) –

Do you remember the uproar in the news when Sony's PlayStation Network was hacked? Here are some tidbits that were offered up as article teasers by MSNBC at the time:

- Sony said on Saturday it had removed off the Internet the personal details of 2,500 people that had been stolen by hackers and posted online. PlayStation Network restart delayed.
- The massive data breach at Sony Corp.'s PlayStation Network has left accountholders worrying that their credit card information could fall into the wrong hands. Now the technology giant is hoping to ease concerns by offering free identity theft protection to affected customers.
- Sony has won over some gamers by offering free access to its PlayStation Network to compensate for the leak of personal details on 78 million user accounts, but still has some way to go to regain the trust of consumers. Source

Wow! That was a nightmare for Sony and thousands and thousands of consumers. What happened with Sony "offering free identity theft protection to affected customers"? Sony actually did that; however, the sign-up deadline was June 18, 2011.

That's only one company. Dozens and dozens are hacked each year. Major leaks occur. We see them in the headlines over and over and over. It's a real problem requiring action to prevent and mitigate losses and damages.

Sensitive Data in Multiple Locations

More and more, we (as consumers, businesses, and other organizations) are giving out, collecting, and storing sensitive data of all types – sensitive data that if it falls into the wrong hands, can be a major headache to clear up. That's why Sony offered the identity-theft protection program and why you should have your own identity-theft protection before the horse is out of the barn – before cyber thieves get hold of your customers' and clients' information and before your own personal data is compromised.

Constant Crime

Here's what the US Justice Department has said about cyber crime:

> In the United States and Canada, for example, many people have reported that unauthorized persons have taken funds out of their bank or financial accounts, or, in the worst cases, taken over their identities altogether, running up vast debts and committing crimes while using the victims' names. In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore his reputation in the community and correcting erroneous information for which the criminal is responsible.
>
> [...]
>
> With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes: for example, false applications for loans and credit cards, fraudulent withdrawals from bank accounts, fraudulent use of telephone calling cards, or obtaining other goods or privileges which the criminal might be denied if he were to use his real name. If the criminal takes steps to ensure that bills for the falsely obtained credit cards, or bank statements showing the unauthorized withdrawals, are sent to an address other than the victim's, the victim may not become aware of what is happing until the criminal has already inflicted substantial damage on the victim's assets, credit, and reputation.

Growing Caseload

Here are some examples:

site and using those data to apply for a series of car loans over the Internet.

A. Central District of California. A woman pleaded guilty to federal charges of using a stolen Social Security number to obtain thousands of dollars in credit and then filing for bankruptcy in the name of her victim. More recently, a man was indicted, pleaded guilty to federal charges and was sentenced to 27 months' imprisonment for obtaining private bank account information about an insurance company's policyholders and using that information to deposit $764,000 in counterfeit checks into a bank account he established.
B. Central District of California. Two of three defendants have pleaded guilty to identity theft, bank fraud, and related charges for their roles in a scheme to open bank accounts with both real and fake identification documents, deposit U.S. Treasury checks that were stolen from the mail, and withdraw funds from those accounts.
C. Middle District of Florida. A defendant has been indicted on bank fraud charges for obtaining names, addresses, and Social Security numbers from a Web
D. Southern District of Florida. A woman was indicted and pleaded guilty to federal charges involving her obtaining a fraudulent driver's license in the name of the victim, using the license to withdraw more than $13,000 from the victim's bank account, and obtaining five department store credit cards in the victim's name and charging approximately $4,000 on those cards.
E. District of Kansas. A defendant pleaded guilty to conspiracy, odometer fraud, and mail fraud for operating an odometer "rollback" scheme on used cars. The defendant used false and assumed identities, including the identities of deceased persons, to obtain false identification documents and fraudulent car titles.

Do you work with sensitive customer-or-employee information on any computer network, website, or via any social media? If so, then you need a Plan and Insurance Coverage.

Your Plan

- Make sure your plan meets government mandates.
- Verify the security measures of your ISP, website host, cloud host, etc.
- Harden your website and network.
- When was the last time you requested free annual copies of your credit reports? You can do that online at the websites of the reporting bureaus:
  - Equifax http://www.equifax.com
  - Experian (formerly TRW) http://www.experian.com
  - Trans Union http://www.tuc.com
    If you see anything wrong, you can file your statement online and take other actions to clear any mistakes including those that may indicate some level of misuse of your identity. There are monitoring and notification services available too.
- Be sure your anti-virus and firewall hardware and software are adequate and up-to-date.
- Also see Hill & Usher's articles on the wide subject of Cyber Crime.

This is by no means an exhaustive list. It is meant to highlight the main areas and to stimulate thought and action.

- If you are hit by identity theft or want more information on how to prevent it, here are some pointers and a good source: Privacy Rights Clearinghouse http://www.privacyrights.org/identity.htm
  - Report it. Here's a starter list to consider. Applicability will vary:
    - Local police department
    - Insurance agency / Insurance claim
    - Federal Trade Commission (FTC) http://www.ftc.gov/bcp/edu/microsites/ The FTC is the main federal agency that takes identity-theft reports. They've reported that **approximately 9 million Americans per year are victims of identity theft**.
    - Postal Inspection Service https://postalinspectors.uspis.gov/form
    - Social Security Administration http://www.ssa.gov/oig/guidelin.htm
    - Internal Revenue Service http://www.irs.gov/privacy/article/0,,id
    - If your driver's license was stolen, contact your state's driver's license bureau.
    - If your Passport was stolen, contact the State Department http://www.travel.state.gov/
  - Have a list of all your ID cards and photocopy them all (front and back). Store the copies in a very safe location.
  - Don't forget to check with the credit agencies again too.
  - You should also have list of all your financial-related accounts handy so you may contact each of them.
  - A good idea is to login everywhere and change your passwords before the crooks do. After the financial accounts, go through everywhere else you log in if you believe the thieves may have obtained your user name and password. Prioritize your work. Start where the crooks could do the most damage. If you telecommute, be sure you protect your workplace ASAP.
  - If you lost your credit card numbers, you'll need to follow the instructions of the issuers. Prompt notification is a good idea even if your liability will be limited to $50.
- Be Covered.

Identity-Theft Insurance

I. An Identity Recovery Help Line
II. Case Management Services

scam is used to obtain data from employers or obtain illegal work

III. Expense Reimbursement Insurance

Coverage may often be added to existing or new homeowners, condo, or renters insurance policies and may vary depending upon the state in which you live or operate a business or other organization.

It can help in the following cases and more:

1. **Criminal identity theft** where the stolen identity is used when the criminal is 1) questioned or 2) arrested for another crime (this can cause all sorts of difficulties when applying for work or credit or a passport, etc.)
2. **Employment identity theft** where an employment
3. **Financial identity theft** where the criminal uses the stolen identity to make purchases of goods or service or rent property and such
4. **Identity cloning** where a criminal assumes the identity of the victim full-time, as if there were two of the same person
5. **Medical identity theft** where the thief uses the stolen identity to obtain drugs or medical services (making a mess of health and financial records – sometimes triggering an arrest warrant against the victim of the identity theft, adding insult to injury)

It can take months, even years, and tens of thousands of dollars fully to restore a compromised identity. Be prepared. Let Hill & Usher start helping you today.

Contact Us Now

Hints:
In newer versions of Adobe Reader and Adobe Acrobat:

1. Save your work-in-progress: Menu > File > Save.
2. Menu > Edit > Preferences > Forms > Auto-Complete > Basic: "The basic auto-complete feature stores the information you enter into form fields and uses these entries to suggest relevant choices as you type into a field. Once you enter a character into a field, a drop-down box displays a list of only the most probable matches. Double-click or press Down Arrow in an empty field to display an even larger list of possible matches."
3. Menu > Edit > Preferences > Forms > Auto-Complete > Advanced: "The advanced auto-complete feature stores the information you enter into form fields and uses these entries to suggest relevant choices as you type into a field. If there are probable matches for a field, tabbing into that field will automatically display a list of them. If there is a very probable match, it will be entered in the field automatically. Pressing Tab while the pointer is over an entry in the list chooses the entry and moves to the next field."

Date	Month ____ Day ____ Year (yyyy) ____
Customer: If you know your Hill & Usher Account Number, please enter it now. Otherwise, skip to the next section.	

Attached to Pre-existing First Named Insured (if any)

Full Legal Name	

Primary Contact

Primary Contact data already on file with Hill & Usher	◉ Yes ○ No If "Yes" and if you've entered above 1) the applicable Hill & Usher Account Number or 2) the full legal name of the Pre-existing First Named Insured, then skip the rest of this Primary Contact section, enter any desired remarks, and submit the form. If you are unsure of any applicable Hill & Usher Account Number or whether there is a Pre-existing First Named Insured, please fill out this Primary Contact section.

Type	○ First Named Insured ○ Co-Insured ○ Other ◉ Not Selected
First Name	
Middle Initial	
Last Name	
Home Telephone (10 digits)	
Cell (10 digits)	
Business Telephone (10 digits)	
Fax (10 digits)	
Email	
Preferred Method for Contact	○ Home Phone ○ Cell ○ Business Phone ○ Email ◉ Not Selected
Contact at Work	○ Contact at work anytime ○ Contact at work only for emergencies ○ Never attempt to contact at work under any circumstances ◉ Not Selected
Remarks	I've read Hill & Usher's article, "Identity Theft 2.0" (Identity Theft-081611a.pdf), and wish Hill & Usher to contact me to help develop an Identity-Theft Protection Plan.

In newer versions of Adobe Reader and Adobe Acrobat, save your completed form before submitting:
Menu > File > Save.

SUBMIT

If you have any computer/technical questions/problems with this form, please email our webmaster or call our office @ 800·956·4220
- Monday through Friday, from 8AM to 5PM, Arizona time -

Hill & Usher Insurance & Surety, LLC.
3033 North 44th Street
Suite 300
Phoenix, Arizona 85018

Email: sales@hillusher.com

Phone: 800·956·4220
Fax: 602·956·4418

Identity Theft-081611a.pdf