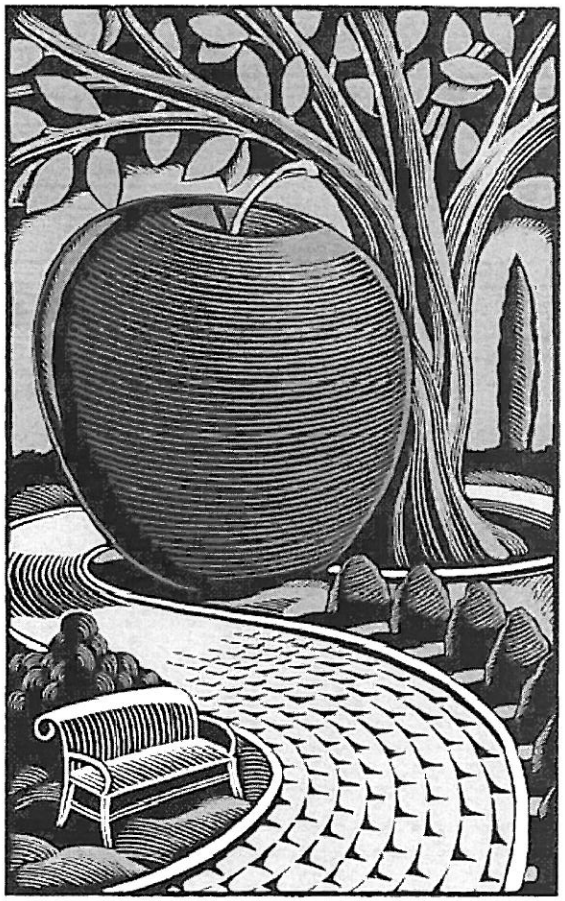
LOWRY HILL



AVOIDING AN IDENTITY CRISIS:

Potential Risks to Your Personal Information and "How to's" for keeping it safe

JASON ANDERSON, CHIEF TECHNOLOGY OFFICER
KATHY KUEHL, FINANCIAL PRINCIPAL

Chicago Estate Planning Council
April 21, 2010

OBJECTIVES

- Background and economic impact
- Different types of identity theft and their ramifications
- Steps you can take to reduce your risk
- What to do if you become a victim

IDENTITY THEFT'S ECONOMIC IMPACT

- Over 11 million Americans were victimized in 2009.
- The average loss is approximately $3,500.
- The average amount of time spent rectifying problems associated with identity theft is 25 hours.
- The economic cost to the U.S. exceeds $50 billion.
- Department of Justice and Federal Trade Commission cite financial fraud as one of the greatest threats to our nation.
- On average, an identity can be purchased online for as little as $10.

Source: *2010 Identity Fraud Survey Report* & www.IdentityTheft.info

TOP 10 STATES FOR IDENTITY THEFT COMPLAINTS

1. Arizona
2. California
3. Florida
4. Texas
5. Nevada
6. New York
7. Georgia
8. Illinois
9. New Mexico
10. Colorado

Source: *Consumer Sentinel Data Book of the Federal Trade Commission* for 2008

HOW DOES IDENTITY THEFT OCCUR?

- Financial/Personal Information Theft
  - Theft of purse or wallet, dumpster diving and stealing contents of mailboxes
  - Obituary searches, "shoulder surfing" and "skimming"
  - Compromised information at work, home or place of business
  - Social Security number identity theft
  - Medical identity theft
  - Criminal identity theft
  - Senior citizen identity theft
  - Children and identity theft

HOW DOES IDENTITY THEFT OCCUR? (CONT.)

- Use of computers/electronics
  - Theft of portable computing devices that have advanced computing capabilities and extensive data handling features
  - Electronic data hijacking via WiFi networks (e.g., "man in the middle" impersonations), Bluetooth, and mal/spyware (e.g., viruses, rootkits, worms)
  - Hackers sourcing more attacks within search engines, social networks, and web-based ads, leveraging unpatched software and seeking gullible and non-detail-oriented individuals
  - Employment of botnets to harvest information via phishing, spearphishing, whaling, spoofing and other Internet-based scams

SPAM'S CURRENT IMPACT

- 90.7 percent of e-mail messages transmitted over the Internet were spam.
- 1 in approximately 360 e-mail messages contained malware.
- 1 in approximately 510 e-mail messages comprised a phishing attack.
- 39.9 percent of the blocked malicious Internet domains were new in March 2010.
- 14.9 percent of all blocked web-based malware was new in March 2010.
- Industrial espionage continues to become more targeted (e.g., spearphishing and whaling) and seeks access to sensitive data stores (e.g., credit card databases).
- Ten largest botnets account for 80 percent of the Internet spam totaling 135 billion messages daily.

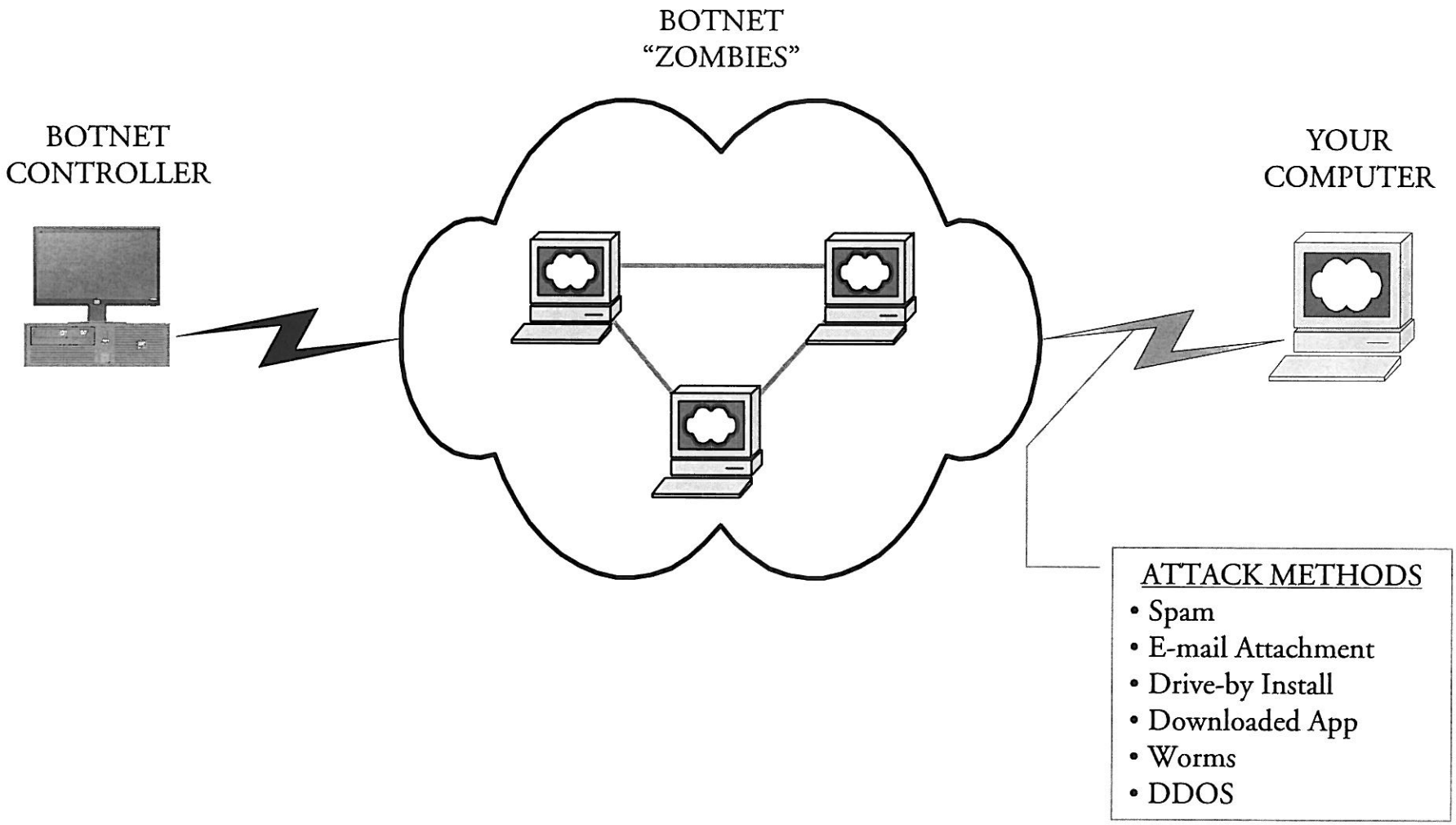
Source: Message Labs *March 2010 Intelligence Report* & http://news.cnet.com/8301-27080_3-20000898-245.html?tag=mncol;title

"SOME" NOTORIOUS BOTNETS

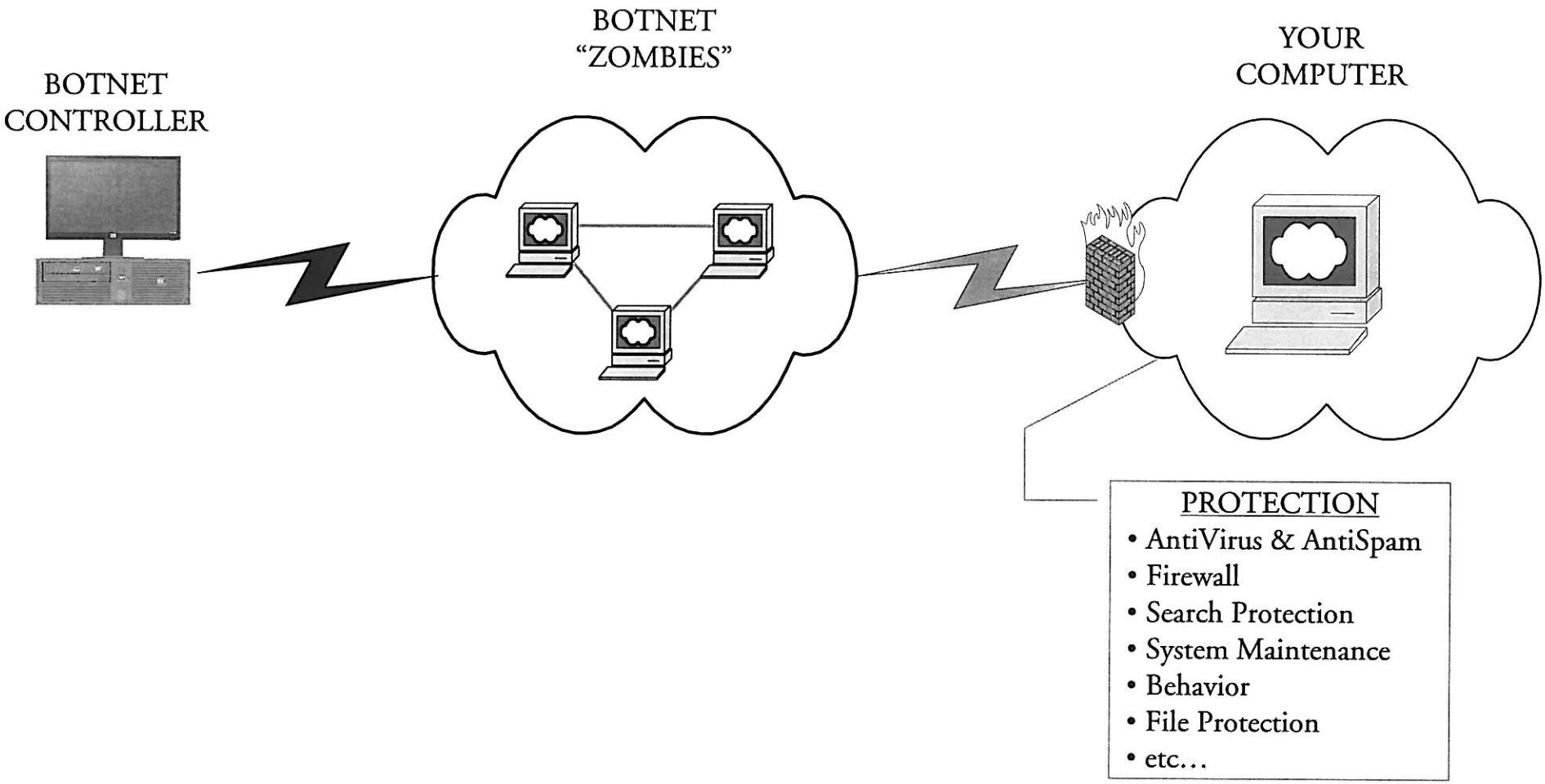
BOTNET	KEY STATS
Grum (aka 0 Tedroo)	• A rootkit Botnet touted as the future of Botnets • Estimated members relatively small at approximately 600,000 bots • Accounts for approximately 25 percent or 40 billion <sic> spam messages/day
Bobax (aka Kraken, Oderoor)	• Believed to be for hire • Estimated members "small" at approximately 100,000 • Accounts for 27 billion spam messages/day
Rustock (aka Costrat)	• Believed to have the largest membership at approximately 2 million bots • Known for delivering image-based spam of legitimate newsletters as a means of thwarting anti-spam filters •Can send encrypted Spam to thwart initial filters
Donbut (aka Costrat)	• First known Botnet to use URL shortening
URLZone	• Estimated members around 6,000 • Most advanced banking Botnet to date
Zeus (aka Kneber)	• Steals account data and can post online-banking, ACH and payroll transactions • Sophisticated modular architecture that is for purchase • Very lucrative with high ROI

Source: http://blogs.techrepublic.com/10things/?p=1373, MessageLabs *February 2010 Intelligence Report* & Finjan *Cybercrime Intelligence and Cisco Systems Annual Security Report* for 2009.

BASIC ANATOMY OF A BOTNET



BASIC BOTNET DEFENSE



WHAT CAN THE THIEF DO WITH YOUR INFORMATION?

- Open new credit card accounts in your name
- Call credit card issuer and change billing address on your account
- Open bank accounts and write bad checks
- Counterfeit checks, credit or debit cards and authorize electronic transfers
- Establish phone or wireless service in your name
- Buy cars, appliances and other large purchases
- Obtain identification with his/her picture and your name
- Give your name to police during an arrest
- File bankruptcy under your name

REDUCING YOUR RISK

- ✓ Safeguard your personal information and monitor your accounts
- ✓ Obtain regular copies of your credit report
- ✓ Shred physical documents, CDs, credit cards (anything that contains confidential information)
- ✓ Use your own computer for online business
- ✓ Use a credit card instead of a debit card for purchases (especially online purchases)
- ✓ Consider using one credit card and one e-mail address for all online transactions
- ✓ Shop online only at secure websites ("https")
- ✓ Limit the posting of personal information wherever possible (e.g., in obituaries, chat rooms, social networking websites, blogs, résumé/job websites, etc.)
- ✓ Use strong passwords

SOCIAL NETWORKING

SOPHOS Facebook ID Probe 2009 results:

- 43 percent of recipients accepted unknown friend requests.
- 73 percent of recipients provided full dates of birth.
- 22 percent of recipients provided partial dates of birth.
- 94 percent of recipients provided their e-mail addresses.
- 48 percent of recipients provided their present colleges or workplaces.
- 46 percent of recipients provided their towns of residence.
- 38 percent of recipients provided some form of family/friend data.

Recommended resource

- http://www.sophos.com/security/best-practice/facebook/

Source: http://www.sophos.com/blogs/duck/g/2009/12/06/facebook-id-probe-2009/

REDUCING YOUR RISK (CONT.)

- ✓ Notify your bank and/or credit institution in advance of traveling out of the country.
- ✓ When out of town for an extended period of time:
  - ➢ Have someone watch your residence and continue its external maintenance.
  - ➢ Stop your mail and newspaper from being delivered.
- ✓ Minimize amount of personal information you carry when traveling.
- ✓ Take the time to read and understand the privacy policies of online vendors.
- ✓ Be wary of clicking on website addresses.
  - ➢ Don't click on a link provided in an email.
  - ➢ Visually verify the link when clicking on the results of web searches.

REDUCING YOUR RISK (CONT.)

- ✓ Install modern AntiVirus software on your computer, and set it to update its definitions daily.
- ✓ Install modern AntiMalware/Spyware software on your computer, and set it to update its definitions daily.
- ✓ Install a modern software firewall on your computer, and set it to update its definitions daily.
- ✓ Install operating system (e.g., Microsoft Windows), web browser and key application (e.g., Microsoft Office, Adobe Acrobat) patches promptly.
- ✓ Setup your wireless network securely.
- ✓ Encrypt confidential information.
- ✓ Frequently backup your computer.
- ✓ Safely dispose of old computer equipment using a DOD grade 52202.22-M wiping utility.
- ✓ Monitor your online identity and reputation.

WHAT TO DO IF YOU BECOME A VICTIM

1. Assess the initial impact of the identity theft. (What type of data was lost? Which accounts are at risk? etc.)
2. If possible, determine how the breach occurred (Has your computer had a virus recently?)
3. Gather any information that may be helpful in relaying the breach to the proper authorities (e.g., credit card numbers, bank accounts).
4. Prepare to contact the various institutions that will assist in recovering from the breach (e.g., police, credit bureaus, financial institutions, Federal Trade Commission).
5. Contact security/fraud departments of institutions where your accounts are held.
6. File an *Identity Theft Report* with the police within 72 hours of realizing you've been victimized, and obtain a copy for your records.
7. Document conversations, and keep copies of all documents and written correspondence.
8. Alert credit bureaus.

WHAT TO DO IF YOU BECOME A VICTIM (CONT.)

9. File a complaint with the FTC.
10. Contact other potentially impacted institutions.
11. Change your impacted security credentials (e.g., e-mail addresses, credit card Pins, online banking).
12. Contact your immediate family or other relevant individuals.
13. Consider placing a *credit freeze* on your file with the credit bureaus.
14. Review and adjust (e.g., install and keep updated antivirus software, limit information posted online).
15. Monitor your situation and financial statements.
16. Find victim support through various resources (e.g., FTC, Identity Theft Resource Center).

FRAUD ALERT VERSUS CREDIT FREEZE

Fraud Alert

- Requires creditor to contact you before issuing credit in your name
- Free of charge
- Two types: Initial Alert and Extended Alert
  - Initial Alerts are appropriate when you sense that you may have been a victim of identity theft (e.g., if your wallet was stolen or you have fallen for a phishing scam). This type of alert does not require proof that you are a victim.
  - An Extended Alert is appropriate when you have been a victim of identity theft. To file for this type of alert, you will need to provide proof in the form on an *Identity Theft Report*.

Credit Freeze

- Prevents perpetrators from opening accounts in your name
- Also prevents potential creditors or loan officers from checking your credit file
- $10 fee (usually) per credit bureau to initiate, $10 fee to lift freeze (no fee for victims of identity theft)
- Varying laws surrounding credit freezes from state to state

SUMMARY

- Everyone is at risk of having their personal information compromised.
- There are many different ways your identity can be stolen.
- Take precautionary steps to protect yourself, and know what to do in the event you become a victim.

APPENDIX: RESOURCES

Identity Theft Laws in Illinois:

- Identity Theft Laws – 720 Ill. Comp. Stat. 5/16g, 2006 PA 94-0827
- Information Breach Law – HB1633
- Spam Law – 815 ILLS 511/1
- Credit Freeze Law – 815 ILLS 502/2MM (effective January 1, 2007)

Contacts in Illinois:

- Attorney General's Office (312) 814.3000 (http://illinoisattorneygeneral.gov)
- AG's ID Theft Hotline 1.866.999.5630
- Illinois Department of Motor Vehicles (www.dmv.org)

APPENDIX: RESOURCES

General Identity Theft Resources:

- Federal Trade Commission's ID Theft Microsite: http://www.ftc.gov/bcp/edu/microsites/idtheft/
- Identity Theft Resource Center: www.idtheftcenter.org
- National Cyber Security Alliance: www.staysafeonline.org
- Fight Identity Theft: www.fightidentitytheft.com

Credit Bureau Websites:

- Equifax 1.800.685.1111 (www.equifax.com)
- Experian 1.888.397.3742 (www.experian.com)
- TransUnion (www.transunion.com)
  - Free annual credit report: 1.877.322.8228
  - Credit report disputes: 1.800.680.7289
  - Fraud Victim Assistance Department: 1.800.680.7289
- www.annualcreditreport.com
  - Website created by the credit bureaus to help streamline the credit review processs

APPENDIX: RESOURCES

How to Opt Out:

- Opting out of Pre-Screened Credit Offers: call 1.888.5OPTOUT (1.888.567.8688) or visit www.OptOutPreScreen.com
- Opting out of the Direct Marketing Assocation: www.dmachoice.org/consumerassistance.php
- Opting out of Telemarketing Phone Calls: call 1.888.383.1222 or visit the National Do Not Call Registry at www.donotcall.gov/default.aspx

Identify Theft Protection Services – Prices and Reviews:

- www.nextadvisor.com

APPENDIX: FOR MORE INFORMATION

Jason Anderson
Chief Technology Officer
Lowry Hill
90 South Seventh Street, Suite 5300
Minneapolis, MN 55402
612.667.1790
janderson@lowryhill.com

Laura Clark
Investment Principal
Lowry Hill
980 North Michigan Avenue, Suite 1400
Chicago, IL 60611
312.214.6309
lclark@lowryhill.com

Kathy Kuehl
Financial Principal
Lowry Hill
90 South Seventh Street, Suite 5300
Minneapolis, MN 55402
612.316.2690
kkuehl@lowryhill.com

APPENDIX: DISCLOSURES

This presentation is for informational purposes only and does not constitute legal advice. Discussions or answers to questions during the presentation should also not be relied upon as legal advice. This presentation includes data that shall not be duplicated, used, or disclosed—in whole or in part—for any purpose outside the audience to whom it is being presented. Lowry Hill does not and cannot guarantee that by using this information you will not be a victim of identity theft nor that the information provided here is relevant to your particular situation. By using the information provided here, you understand you are using this information at your own risk. The information is "As is," "With all faults." User assumes all risk of use, damage, or injury.

The laws discussed in this presentation are, like most laws, constantly amended and interpreted through legal and social challenges. You are encouraged to review the laws and draw your own conclusions through independent research.

LOWRY HILL

SECURE COMPUTING GUIDELINES

Maintaining a secure computing environment is all about layers, maintenance and behavior. For example, it is imperative to implement countermeasures that address the layer at which each computing service runs. Here, a computing service can be as simple as your web browser, your internet connection or your e-mail program and a countermeasure can be something you install and/or a practice you follow.

The information and product recommendations provided below are by no means complete. Computing security changes too frequently, and individual needs are too varied to meet this goal in this space alone. All recommendations are based on a combination of internal experience, internal research and industry-based best practices. Finally, Lowry Hill was not paid for any product recommendation and does not warrant their functionality nor support their implementation.

	BASIC PROTECTION						ADDITIONAL PROTECTION				
PRODUCT NAME	ANTI-MALWARE	ANTI-SPAM	SOFTWARE FIREWALL	PATCH MONITOR	BACKUP	WEBSITE SCREEN	SYSTEM MONITOR	SYSTEM CLEANUP	FILE/DISK ENCRYPTION	PASSWORD MANAGER	HARDWARE FIREWALL
Acronis TrueImage					●						
Ad-Aware Pro 8.1	●										
Avast! Free AntiVirus	●										
CCleaner*								●			
Comodo AntiSpam*		●									
Comodo AntiVirus*	●										
Comodo Firewall*			●								
Comodo Internet Security*	●		●								
LinkSys Firewall Router											●
McAfee AntiVirus Plus 2010	●					●					
McAfee Internet Security 2010	●	●	●		●	●		●			
McAfee SiteAdvisor*						●					
McAfee Total Protection 2010	●	●	●		●	●		●	●		
NetGear Firewall Router											●
Norton 360 v 4	●	●	●		●	●		●		●	
Norton AntiVirus 2010	●										
Norton Ghost 14 or 15					●						
Norton Internet Security 2010	●	●	●			●				●	
OpenDNS*	●					●					
Secunia PSI*				●			●				
Spyware Doctor with AntiVirus 2010	●										
TrendMicro RUBotted*							●				
TrueCrypt*									●		
Web of Trust*						●					
WebRoot Window Washer								●			
WinPatrol*							●				
ZoneAlarm Pro			●								

NOTE 1: There may be limitations in the products above that will not meet your needs. For instance, the McAfee Total Protection 2010 backup option is online only and limited to 2GB of storage. The Norton backup options, on the other hand, support both local and online backups (with varying amounts of storage capacity). Please review all products features and requirements before purchasing and installing.

*NOTE 2: * Denotes free software when used for home use.*

NOTE 3: The product names in blue text denote the software used in the presenter's home network.

PRODUCTS & PRACTICES THAT CAN HELP SECURE YOUR COMPUTER

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
AntiMalware Software (includes spyware, virus, rootkit, trojan... detection, protection and eradication)	➢ Norton 360 v.4 ➢ Norton Internet Security 2010 ➢ McAfee Total Protection 2010 ➢ McAfee Internet Security 2010 ➢ Avast! Free AntiVirus (FREE at www.avast.com) ➢ Ad-aware Pro 8.1 ➢ Comodo Internet Security (FREE at www.comodo.com) ➢ Comodo AntiVirus (FREE at www.comodo.com) ➢ F-Secure Blacklight (FREE at http://www.f-secure.com/blacklight/) ➢ Microsoft RootKitRevealer (FREE at technet.microsoft.com/en-us/sysinternals/bb897445.aspx) NOTE 1: Not all anti-malware vendors classify malware in the same manner. Consequently, results will vary from one vendor's product to the next. NOTE 2: Check with your Internet Service Provider as they may provide a software package for free (e.g., as of January.2010, Comcast offers Norton 360 v. 4 for free).	WHAT TO INSTALL From the list at left, install at least one of the following: o Norton 360 o McAfee Total Protection o Norton Internet Security o McAfee Internet Security NOTE: Make sure your AntiMalware software is either the most recently released version or the previously released version. CONFIGURATION ➢ Your AntiMalware software definitions should be updated at least once a day. ➢ Your AntiMalware software should be set to scan your entire hard drive at least twice a week, scan any "accessed" file in real time and, if possible, scan your e-mail's inbox. ➢ When using the most recently released version, make sure it has been on the market for at least four months before installing it. This will give the vendor time to address issues.
AntiSpam	➢ Norton 360 v.4 ➢ Norton Internet Security 2010 ➢ McAfee Total Protection 2010 ➢ McAfee Internet Security 2010 ➢ Comodo AntiSpam (FREE at www.comodo.com)	WHAT TO INSTALL ➢ If you select one of the Norton or McAfee products as your AntiMalware software, use it as your AntiSpam software, too. ➢ Your ISP, web e-mail provider (if you use one) and/or installed e-mail client software (e.g., Outlook, Apple Mail) may offer AntiSpam services. If so, use those in conjunction with one of the products at left. CONFIGURATION ➢ Your AntiSpam software definitions should be updated daily. ➢ Your AntiSpam software should check message on arrival. ➢ Make sure your AntiMalware software is either the most recently released version or the previously released version.

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
Software Firewall	➢ Norton 360 v. 4 ➢ Norton Internet Security 2010 ➢ McAfee Total Protection 2010 ➢ McAfee Internet Security 2010 ➢ ZoneAlarm Pro Firewall 2010 ➢ Comodo Firewall (FREE at www.comodo.com) NOTE: Check with your Internet Service Provider, as they may provide a software package for free (e.g., as of January 2010, Comcast offers Norton 360 v. 4 for free).	WHAT TO INSTALL ➢ If you select one of the Norton or McAfee products as your AntiMalware software, use it as your Firewall software, too. ➢ Your operating system (e.g., Windows 7, Mac OS X, etc.) almost certainly comes with a basic firewall. Using one of the firewalls to the left is an enhancement because the vendors add signature detection that helps thwart malicious traffic attempting to traverse what is normally a trusted Internet traffic channel. For example, a standard firewall may allow all e-mail traffic to take place whereas a software firewall enhanced with behavior analysis may detect malware in transit and cease the communication prior to any damage being done. CONFIGURATION ➢ Your Firewall software definitions should be updated at least daily. ➢ When using the most recently released version, make sure it has been on the market for at least four months before installing it. This will give the vendor time to address issues.
Software Patch Monitoring	➢ Secunia PSI (FREE at secunia.com/vulnerability_scanning/personal)	BEST PRACTICE ➢ Patch all installed software within a few days of the patches release.
Backup Software	➢ Norton 360 v.4 ➢ Norton Ghost 14 (or newer) ➢ Acronis True Image (www.acronis.com)	WHAT TO INSTALL ➢ If you selected Norton 360 as your AntiMalware software, use it as your Backup software, too. ➢ Even though you are installing backup software, leave the Restore Point functionality enabled on Windows-based computers. This will provide a quicker operating system recovery, and the full backup can then be used to restore your custom files (e.g., iTunes music, Word docs) after the system has been restored. CONFIGURATION ➢ Backups of your system and critical files should reflect the frequency in which your data changes. At a minimum, backup your data before you install new software and/or have made significant changes to your important data. ➢ Store the physical backup media in a location that is different than your original data source (e.g., a safe deposit box).

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
Website Screening	➢ McAfee's Site Advisor (FREE at www.siteadvisor.com) ➢ Norton 360 v. 4 ➢ Norton Internet Security 2010 ➢ McAfee Total Protection 2010 (includes Site Advisor) ➢ Web of Trust (FREE at www.mywot.com) ➢ OpenDNS (FREE at www.opendns.com)	WHAT TO INSTALL ➢ Setup your Internet connection to use OpenDNS category filtering and install one of the other products. BEST PRACTICES ➢ Visit trusted, reputable websites, and do not download software from untrusted sources. ➢ If you use Firefox, employ NoScript (FREE at http://noscript.net/) to limit untrusted websites' ability to run scripts on your computer. ➢ Avoid websites that end in .hk, .cn, .ph, .ro, .ru and .info. For example: www.acme.cn. ➢ You can manually research a website's legitimacy by leveraging: o The Google Safe Browsing report at http://www.google.com/safebrowsing/diagnostic?site=****. NOTE: To use the service, enter the URL in your browser and replace the **** with your desired website. For example: http://www.google.com/safebrowsing/diagnostic?site=www.lowryhill.com o The McAfee Site Advisor report from the toolbar or, if the toolbar is not installed, at http://www.siteadvisor.com/.
System Monitoring Software	➢ TrendMicro RUBotted (FREE at www.trendsecure.com/portal/en-US/tools/security_tools/rubotted) ➢ WinPatrol (FREE at www.winpatrol.com/download.html) ➢ Secunia PSI (FREE at secunia.com/vulnerability_scanning/personal)	WHAT TO INSTALL ➢ Install at least one of these products: o TrendMicro RUBotted o WinPatrol ➢ And install Secunia PSI

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
System Cleanup	➢ CCleaner (FREE at www.piriform.com) ➢ WebRoot Window Washer ➢ Norton 360 v.4 ➢ McAfee Total Protection 2010 ➢ McAfee Internet Security 2010	WHAT TO INSTALL ➢ Regardless of the AntiMalware product you selected, install one of these products to assist with secure file deletions and manually initiated cleaning processes: o CCleaner (FREE at www.piriform.com) o WebRoot Window Washer CONFIGURATION ➢ Setup or manually run at least weekly scrubs of your unneeded temporary files. ➢ Set the software so that it deletes your files using at least a DOD grade wiping process. This is especially important when using a laptop or netbook.
Hard Disk Encryption	➢ PGP Whole Disk Encryption (www.pgp.com) ➢ TrueCrypt (FREE at www.truecrypt.org) ➢ Bitlocker (part of Windows Vista Ultimate and Windows 7 Ultimate, requires TPM (described below)) ➢ Trusted Platform Model (or TPM) is a hardware-based solution offered by some hardware vendors on select computers (e.g., HP business laptops) ➢ Seagate encrypted FDE hard drive (These are new, so please check the vendor's computer to see if the technology is embedded.)	BEST PRACTICES ➢ If your computer's hard drive contains any confidential information (e.g., social security numbers, account numbers) store the data in an encrypted vault that supports, at a minimum, 128 bit AES encryption (preferably 256 bit AES encryption). ➢ When encrypting your data, the password should be at least 24 characters long and conform to the character variability discussed in the *Passwords* section. ➢ If your computer contains confidential information and is encrypted, unmount the encrypted drive when not in use.
Hardware Firewall Router	➢ NetGear (www.netgear.com) ➢ LinkSys (www.linksys.com or www.cisco.com)	BEST PRACTICE ➢ For any always on Internet connection (e.g., DSL, cable modem), install a hardware firewall between your computer(s) and the modem. This should be done in addition to a software firewall. ➢ Almost all hardware firewalls will provide decent protection out of the box. ➢ Remember to create a new and complex Administrator password for the device.

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
Web Browsers	➢ For Windows XP, Vista or 7, use one of these browsers (in preferred order): o Internet Explorer 8 o Firefox 3.6 (FREE at www.mozilla.com) o Google Chrome 4 (FREE at www.google.com/chrome) ➢ For Macintosh, use Firefox 3.6 ➢ For Ubuntu Linux, use Firefox 3.6.	CONFIGURATION ➢ A great article about securing your web browser can be found at: http://www.us-cert.gov/reading_room/securing_browser/ ➢ Make sure the browser's anti-malware features are enabled (e.g., *SmartScreen* filtering in Internet Explorer 8 (IE 8), Pop-up blocking). NOTE: The effectiveness of IE 8's *SmartScreen* technology is why IE 8 is listed as the preferred browser for Windows platforms. BEST PRACTICES ➢ Quickly update your browser software whenever a new patch is published. ➢ Do not let the website nor the browser save your respective website passwords. Instead, use a third-party product that secures the stored information. ➢ Surf in Private mode if/when possible. ➢ Open a brand new browser session before starting any sensitive online transactions (i.e., reading web e-mail, using online banking). Once completed, log off of the website, and close the browser. ➢ If you use Firefox, employ NoScript (FREE at http://noscript.net/) to limit untrusted website's ability to run scripts on your computer.

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
Operating Systems	➢ For PC systems, use Windows 7. It is more secure than its predecessors, and the performance issues have been cleared up. ➢ For Macintosh systems, OS X Snow Leopard and the older Leopard are your best options. ➢ For Linux systems, the Ubuntu 9.10 (or newer) operating system is a great, user-friendly choice that is free.	SECURITY BEST PRACTICES ➢ Install the latest patches (also known as Hot Fixes and/or Service Packs) at least monthly. For Windows PCs, these patches are available via the *Windows Update* feature universally found under Internet Explorer's menu bar under the *Tools* header. Macintosh updates can be downloaded by the Apple *Software Update* utility. ➢ Setup user accounts for administering your system and accounts for performing daily tasks. ➢ Turn off your computer when it is not in use. If you don't want to turn it off between sessions, lock the system so a password is required to resume operation. ➢ If your computer's hard disk contains confidential information (e.g., social security numbers, account numbers), encrypt it. PERFORMANCE ENHANCEMENT SUGGESTIONS ➢ Add more memory (i.e., RAM). ➢ Make sure your video card is capable of processing your data. ➢ Turn off Startup/AutoRun programs by using a product like *CCleaner*. ➢ Turn off local file indexing services. ➢ Turn off visual enhancements like window animation. ➢ Make sure at least 10 percent of your hard disk's space is free. ➢ Defragment your hard drive with Defraggler (FREE at http://www.defraggler.com) or Diskeeper (www.execsoft.com).

PRODUCTS & PRACTICES THAT CAN HELP SECURE INFORMATION BEYOND YOUR COMPUTER

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
Children and the Internet	➢ OpenDNS (FREE at www.opendns.com) filters malicious websites. ➢ WebWatcher at www.webwatcherkids.com is stealth software that allows you to control and report on Internet usage on a per user basis. It allows for much more granular control than Windows Vista's Parental Controls tool. ➢ Norton Safety Minder at https://onlinefamily.norton.com/familysafety/loginStart.fs is a Norton product that works much like the aforementioned WebWatcher product. It has been free in the past but that may change at any point. ➢ NetNanny at www.netnanny.com is another granular Internet access application that allows you to control and/or monitor what can be accessed on the Internet. ➢ KidZui at www.kidzui.com is a software product that only allows access to Internet-based content deemed appropriate for kids by KidZui reviewers. They offer both free and paid for versions of the product. ➢ Norton Internet Security 2009 and greater offer a free add-on that is functionally similar to Vista's and Windows 7's Parental Controls. ➢ Enable Windows Vista's or Windows 7's Parental Controls. (These are only completely effective if using Microsoft applications).	WHAT TO INSTALL ➢ At a minimum, setup your Internet connection to use OpenDNS category filtering. ➢ Use one of the other products if you believe it is appropriate for the situation. BEST PRACTICES ➢ Place the computer children will use in an open, high-traffic area of your house. ➢ Use an Internet access control package. ➢ Set guidelines so your children know what they can and can't do online. ➢ Know who your child's friends (online and otherwise) are and decide what, if any, chat room monitoring will be undertaken. ➢ If your child participates in a social network (e.g., Facebook, Twitter, MySpace), you may want to review their site(s) from time-to-time. ➢ Teach your child to never give out personal information and to not trust other "friends" blindly. ➢ Know what to do if your child is in danger.

SECURE COMPUTING GUIDELINES

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
Computer Disposal	➢ WebRoot Window Washer at www.webroot.com/En_US/consumer-products-windowwasher.html ➢ Eraser at (FREE at www.heidi.ie/eraser/) ➢ CyberScrub's *cyberCide* Data Destruction at www.cyberscrub.com ➢ DBAN: Darik's *Boot and Nuke* at dban.sourceforge.net (FREE) ➢ WhiteCanyon's *WipeDrive* at www.whitecanyon.com ➢ Some hardware vendors (e.g., HP) offer specific products with built-in disk sanitization capabilities.	BEST PRACTICES ➢ Sanitize all hard drives before disposing of hardware using a method that is rated DOD 5220-22.M. If the drive no longer functions, physically destroy it by deforming any internal disks and smashing any embedded computer chips. Incinerating, if available, is another option. ➢ Remove all personal markings from the device. ➢ Drop the device off at an electronics recycling center.
Online Reputation (Business)	➢ GoolagScanner (at www.goolag.org) is a tool that scans websites and reports what hidden information is being picked up by Google's search engine and, potentially, other unwanted parties. ➢ www.archive.org hosts the WayBack Machine that contains historical copies of websites. It is a good idea to be as familiar with your old content as you are with your current content.	BEST PRACTICES ➢ Perform periodic searches of yourself to ensure that the data posted on the Internet is appropriate and accurate. ➢ Make sure you have clear policies and procedures that describe what is and is not acceptable in terms of working with company information. Follow this work-up with monitoring and annual training.
Online Reputation (Personal)	➢ The Affinion Group (providers of criminal activity to banks) offers Identity Secure (at www.identitysecure.com), a service that can help monitor your online identity and credit information. IdentityGuard (at www.identityguard.com is a close competitor). ➢ www.reputationdefender.com is a service that can help research and correct online material associated/related to you. ➢ www.defendmyname.com helps trim negative search results from appearing.	➢ Assume that "What happens on the Internet stays on the Internet." In other words, assume that the data you have posted on the Internet will exist forever. ➢ If you participate in blogs and/or social networks, limit the posting of personal information and don't trust others blindly. ➢ Perform periodic searches on yourself to ensure that the data that is out there is appropriate and accurate. ➢ With search engines and sites like www.zillow.com be prepared to answer questions from children, family, friends, neighbors, etc. about your career, social and financial standing.

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
Passwords	➢ TrueCrypt (FREE at www.truecrypt.org) ➢ OpenID	USER ID PASSWORDS ➢ Keep all passwords in a safe and secure place. If you have multiple User IDs and passwords, store them in an encrypted vault using *TrueCrypt* or a dedicated password management application that stores the information in an encrypted format. ➢ Do not share your passwords with anyone. ➢ Passwords should not be comprised of a single word found in a dictionary. ➢ Passwords should not be the same across user accounts. ➢ Passwords should be changed at least once every 60 days. ➢ Passwords should not contain personal information that is easy to guess (e.g., your birthday, dog's name, etc.). ➢ Do NOT enable password auto-entry in your applications (e.g., Internet Explorer). ➢ Wherever possible, passwords should be eight characters or longer. For passwords used to encrypt data, they should be 24 characters or longer. An easy way to make a long password is to think of a sentence that means something to you and then add the complexity variables detailed in the next two bullets. For example: *I-wish-I-could-vacation-in-Naples-FL-every-January.* ➢ Passwords should contain both upper and lower case letters, numbers AND special characters (e.g., an asterisk). An example of a good password is: *UpNDown3x!* ➢ An easy way to create difficult passwords is to use a substitution scheme. For example, replacing A, E, I , O and U with 1, 2, 3, 4 and 5 respectively. Using this scheme, a password of *JasonA!* would become *J1s4n1!* ➢ A master password can be used and applied to multiple sites. For example, the base password is *UpNDown3*. When applied to websites the password is then changed slightly per the following examples: o At my banking website, the password is: *UpNDown3Bank!* o For iTunes, my password is: *UpNDown3Tunes!* o For my web-based email, the password is: *UpNDown3Mail!* ➢ When prompted to setup a challenge response that can be used to unlock your account, opt for the custom question and use an answer that isn't factual. For example, the answer to *The name of your high school mascot* could be *SmellyFish.*

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
Personal Digital Assistants (PDA), Cell Phones, MP3 Players…..	➢ Apple iPod, iTouch, iPhone, iPad ➢ Blackberry ➢ Microsoft Zune ➢ Cell Phones	BEST PRACTICES ➢ Treat your PDA like you would a full blown computer. This means make sure you keep its base software up-to-date, make sure you install security software if available and make sure you back it up regularly. ➢ At a minimum, password protect your device (using a complex password, if possible). If available, enable the data encryption features (which will require a password to unlock the device anyway). ➢ If the device's data cannot be encrypted, do not store any confidential data on the device (e.g., do not store passwords, SSN, banking info). NOTE: If you own an iPhone or iTouch, you may want to review the book *iPhone Forensics* by Jonathan Zdziarski and/or check out the author's web posts regarding the ease of which the iPhone (et al) can be hacked. ➢ Ensure that ancillary wireless access (e.g., WiFi, Bluetooth) is disabled unless you require it. When required, turn it on manually and then turn it back off when finished. ➢ Download only reputable software. And before doing so, perform a quick web search to see if the software contains any known security issues. This step is especially important with the iPhone, iTouch and iPad software due to the recent discovery of data harvesting applications with capabilities akin to SpyPhone.
Portable Storage Encryption	➢ TrueCrypt (FREE at www.truecrypt.org) ➢ Lexar USB drives with SecureII software. ➢ Biometric USB drives with encryption that is unlocked via your fingerprint.	➢ When using portable storage media of any kind (e.g., backup tape, key chain drive, PC Card, floppy disk, laptop computer), store the confidential files in an encrypted vault that supports, at a minimum, 128 bit AES encryption (preferably 256 bit AES encryption). ➢ When encrypting your data, the password should be at least 24 characters long and conform to the character variability discussed in the *Passwords* section.

FUNCTION	VENDORS & PRODUCTS	RECOMMENDATIONS & BEST PRACTICES
Wireless Networking	➢ NetGear ➢ LinkSys	Use a wired network whenever possible. If you find that you need a wireless network, the following security measures should be put in place: 1. If possible, use 802.11n or 802.11g networking equipment. 2. If your wireless router has a default name, it should be renamed to something nondescript. *Example: Veggie3* 3. Like the router's name, the wireless router's SSID should be renamed to something nondescript. *Example: Berry4* 4. If possible, the SSID broadcast should be turned off. 5. Your internal network should be based on private addresses. This means that the network should use addresses like 192.168.x.x or 10.x.x.x. Most wireless routers are setup like this by default. 6. Administration access for the wireless router should be limited to only the required internal network addresses (e.g., your main PC). 7. Wireless hardware Admin accounts should be renamed (if possible). 8. Wireless hardware Admin accounts should have a unique password assigned that conforms to the Password recommendations (above). 9. Enable at least WPA (or WiFi Protected Access) security. WEP and other lower-level security protocols should be disabled. NOTE: Your computer's wireless network cards must also support WPA. Otherwise they will not be able to connect to your wireless router. 10. If you are required to provide a security string for your WPA settings, the string should be greater than 24 characters long. *Example (using dashes for spaces and the number 1 for the letter i): The-w1nd-1s-from-the-North-at-34MPH!* 11. Restrict access to your wireless router by specifying only your equipment's MAC addresses. *Example: 00:AA:00:4R:YT:G5* 12. If possible, turn off the wireless access equipment when not in use. NOTE: All devices must support WPA to use it successfully. While the technology is billed as cross-vendor compatible, stick to a single vendor (e.g., NetGear) if possible.

PROCESS RECOMMENDATIONS TO HELP KEEP YOUR INFORMATION SECURE

PROCEDURE	RECOMMENDATIONS
Bluetooth Use	➢ If you don't need Bluetooth functionality, turn it off. ➢ Always pair your devices in a private and isolated area to help prevent eavesdroppers from discovering your PIN. ➢ Set the Bluetooth to non-discoverable mode to avoid Bluejacking and Bluesnarfing. ➢ For more information, see www.bluetooth.com.
Computing in Public	➢ When you work on your computer in a public place (e.g., on an airplane, in a coffee shop) it is important to make sure that you and your equipment are situated such that onlookers cannot see your information. ➢ If possible, never use a publicly available computer (e.g., an Internet café computer or a hotel's business center computer). If you must use one of these computers, never transact personal and/or confidential information (e.g., shop or bank online, check your e-mail, logon to a work resource) while using the computer. ➢ Do not attach any of your equipment (e.g., an iPod, a USB drive) to a publicly available computer. ➢ If you are using a publicly available WiFi network, make sure that at a minimum you follow these guidelines: o Have your computer equipped with products that cover each of the *Basic Protection* categories found on the first page of this document. o If possible, do not transact personal and/or confidential information while connected to the network. If you must transact this type of information, make sure that you are doing so only via a connection that is encrypted between your computer and the required server. For example, if you need to communicate via web-based e-mail, make sure that you are both logging on and using your e-mail via an HTTPS connection (instead of the insecure HTTP connection) that is offered by your web-mail provider. o If the public network provider offers connection software, like that found via Starbucks WiFi provider, make sure you use it as it will usually find and authenticate legitimate networks as opposed to a hacker network attempting to impersonate the legitimate network.
File and Print Sharing	File and print sharing should be turned off whenever possible. In Windows XP, you turn off file and print sharing by: ➢ Open your *Control Panel.* ➢ Open the *Network Connection.* ➢ For each of your active network connections: o Right-click on the network connection icon and select **Properties.** o Deselect the *File and Print Sharing for Microsoft Networks* setting. o Click OK (repeat as necessary for each network connection. In Windows Vista and Windows 7, you turn off file and print sharing by: ➢ Open your *Control Panel.* ➢ Open the *Network and Sharing Center.* ➢ For each sharing option that is not needed, select the Off option.

PROCEDURE	RECOMMENDATIONS
Social Networking, Chat Rooms, Instant Messaging	➢ Remember that what happens on the Internet stays on the Internet. In other words, assume that what you post on the Internet will exist forever. ➢ Generally speaking, limit both the posting and sharing of personal information as much as possible, and don't trust others blindly. ➢ The implications surrounding the use of FaceBook are too numerous to cover in this space. If you do use FaceBook, check out the Sophos FaceBook Best Practices Guide at http://www.sophos.com/security/best-practice/facebook/ for some great information. This guide can help you protect your identity by offering advice on how to setup FaceBook's security settings. ➢ Do not click on any links from unknown sources. If you encounter a link to something that interests you and it's from a trusted source, still use the process by where you copy the link and paste it into another browser window instead of simply clicking on it. Like links found in phishing e-mail, the link you see may not take you to the represented destination. ➢ Do not accept any downloads offered in a chat session. ➢ Make sure you read and understand the Privacy Policies and User Agreements for any of the sites you use.
Working with E-mail	➢ Standard e-mail is like a postcard: anyone who has access to it in transport or in storage can read it. Keep this in mind when composing e-mail to make sure you aren't exposing content you'd rather keep secure or may regret surfacing at a later point in time. ➢ Do not send nor open any eCards. ➢ If you receive an e-mail and you don't know who it's from, delete it. ➢ If you receive an e-mail with an offer that sounds to good to be true, it is. Delete the message. ➢ Use your e-mail program's auto-preview option (the option that shows you the first few lines of the e-mail without opening the actual e-mail). This will give you a good indication of the e-mail's content and legitimacy. Conversely, do NOT use your e-mail program's Preview Pane as this can actually open a message and provide feedback to spammers. ➢ If you receive an e-mail that demands you to react to an urgent matter, odds are the message is a scam. For example, you receive a message stating that you must click a link and validate your FaceBook profile within the next 24 hours or it will be deleted. Delete these messages. ➢ If you can't tell if a message is legitimate and you feel you need to act, directly contact a representative from the institution depicted as the sender. If you do not know a representative, do not rely on the contact information contained in the e-mail. Instead, check the institution's website for contact info. ➢ Be extra suspicious when you receive a message that contains a general greeting and/or a preponderance of misspellings and grammatical errors. ➢ Do NOT click on any links in a message. If you must access an embedded link, copy it from the e-mail and paste it into your web browser's address field. ➢ It is a good idea to avoid opening all attachments, but that is most likely unrealistic. To help filter the good from the bad, use the following risk-ranked list when deciding what to actually open: 1. Do not open any attachment if you do not know the sender. 2. Do not open any attachments that end with exe, bat, cmd, com, htm, html, js, jse, pif, ps1, rar, tar, vbe, vbs, wsh, ws, wsf and zip. 3. If possible, do not open any attachments that end with doc, docx, dot, dotx, ppt, pptx, xls, xlsx, xlt, xltx, or zip from an untrusted source.

PROCEDURE	RECOMMENDATIONS
Green Computing	➢ If you can, turn your computer off when not in use. Otherwise, enable the sleep or hibernate mode to reduce the amount of electricity your computer consumes when not in use. ➢ Use an LCD screen as opposed to a CRT. ➢ Turn off the peripherals (e.g., printers) when not in use.
Opting Out	➢ Opt out of pre-approved credit card offers, insurance mailings or other offers by calling 1-888-5OPT-OUT (or visit www.optoutprescreen.com). ➢ Opt out of phone solicitations at www.donotcall.gov.
Web Browsing	➢ When possible, use your browser's *Private* mode to prevent your activity from being recorded and, subsequently, being read by a future malware infection. ➢ Visit trusted, reputable websites and do not download software from untrusted sources. ➢ Do not download media viewers offered by websites (e.g., a viewer needed to read the lyrics of a song). This is a common way of getting unsuspecting people to install spyware. ➢ Do not download and install security software that is offered by a pop-up ad. ➢ Avoid websites hosted in known malware harbors such as those domain addresses that end in .hk, .cn, .ph, .ro, .ru and .info (for example, www.acme.cn.) ➢ When you aren't using your browser, shut it down. This can prevent malware embedded in an advertisement from infecting your computer when you are away, a situation that can occur if the browser is left on a website that both displays ads and auto refreshes. ➢ After completing a secure online session (e.g., you transferred money at your online banding site), logoff and close the browser. ➢ If you use Firefox, employ NoScript (FREE at http://noscript.net/) to limit an untrusted website's ability to run scripts on your computer.

LISA MADIGAN
ILLINOIS ATTORNEY GENERAL

PLACING A SECURITY FREEZE ON YOUR CREDIT REPORT

As of January 1, 2007, any consumer in Illinois may place a security freeze on his or her credit report by requesting one in writing by certified mail to the credit reporting agency. A security freeze prohibits, with certain specific exceptions, the credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer.

The credit reporting agency may charge up to $10 for each placing, removing or temporary lifting of a security freeze. Senior citizens 65 years of age and older will not be charged to place or permanently lift the security freeze, but may be charged up to $10 for each temporary lifting of a security freeze.

Victims of identity theft will not be charged any fees in connection with the placing, removing, or temporary lifting of a security freeze.

To obtain more detailed information on how to place a security freeze on your credit reports, see below.

HOW TO FREEZE YOUR CREDIT FILES

A security freeze means that your file cannot be shared with potential creditors. A security freeze can help prevent identity theft. Most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and Social Security number probably would not be able to obtain credit in your name.

How do I place a security freeze?

To place a freeze, you must write to each of the three credit bureaus. Credit bureaus charge a $10 fee to place a security freeze, unless you are at least 65 years old, in which case there is no fee. Victims of identity theft will not be charged a fee to place the freeze.

Write to all three addresses below and include the information that follows:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
P.O. Box 6790
Fullerton, CA 92834-6790

For each, you must:

- Send a letter by certified mail;

- If you are a victim of identity theft, you must include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
- Provide your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth;
- If you have moved in the past 5 years, supply the addresses where you have lived over the prior 5 years.
- Provide proof of current address such as a current utility bill or phone bill
- Send a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- If applicable, include payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)

How long does it take for a security freeze to be in effect?

Within five (5) business days after receiving your letter, the credit reporting agencies listed above will place a freeze on providing credit reports to potential creditors.

Within 10 business days after receiving your letter to place a freeze on your account, the credit reporting agencies will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep this PIN or password in a safe place.

Can I open new credit accounts if my files are frozen?

Yes. You can have a security freeze temporarily lifted for a specified period of time or for a specific party. There is up to a $10 charge for either temporarily lifting the security freeze or allowing a specific potential creditor to access your credit report. Victims of identity theft can temporarily lift the security freeze or allow a specific party to access their credit report at no charge. The steps to temporarily lift a security freeze or to allow a specific potential creditor to access your credit report are as follows:

- Contact the credit reporting agencies above.
- The manner by which you contact them is determined by them, but it may be by way of telephone, fax or over the Internet or by mail;
- You must provide proper identification;
- You must provide your unique PIN or password; and
- You must specify during what time period your credit report will be accessible to potential creditors (for example August 1 to August 5,) or for which potential creditor you want the security freeze lifted (for example: Sears.)

How long does it take for a security freeze to be lifted?

Credit bureaus must lift a freeze no later than three (3) business days after receiving your request.

What will a potential creditor who requests my file see if it is frozen?

A potential creditor will see a message or a code indicating the file is frozen.

Can a potential creditor get my credit score if my file is frozen?

No. A potential creditor who requests your file from one of the three credit bureaus will only get a

message or a code indicating that the file is frozen.

Can I order my own credit report if my file is frozen?

Yes.

Can anyone see my credit file if it is frozen?

When you have a security freeze on your credit file, certain entities still have access to it. Your report can still be released to your existing creditors or to collection agencies acting on their own behalf. They can use it to review or collect on your account. Other creditors may also use your information to make offers of credit. Government agencies may also have access in response to a court or administrative order, a subpoena, or a search warrant.

Do I have to freeze my file with all three credit bureaus?

Yes. Different credit issuers may use different credit bureaus. If you want to stop your credit file from being viewed, you must freeze it with Equifax, Experian, and Trans Union.

Will a freeze lower my credit score?

No.

To protect my credit, should my spouse's credit file be frozen too?

Yes.

Does freezing my file mean that I won't receive pre-approved credit offers?

No. You can stop the pre-approved credit offers by calling 888-5OPTOUT (888-567-8688). Or you can do this online at www.optoutprescreen.com. This will stop most of the offers, such as the ones that go through the credit bureaus. The opt out request lasts for five years or you can make it permanent.

What law requires security freezes?

The Illinois security freeze law is located at 815 ILCS 505/2MM.

SAMPLE LETTER TO EQUIFAX – FOR PLACING A SECURITY FREEZE
(MUST BE SENT **CERTIFIED MAIL**)

Date

Equifax
Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Dear Equifax:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one of the following:
I have included a $10 fee to place a security freeze on my credit file

OR

I am a senior (at least 65 years old) and the fee does not apply to me. OR

I am an identity theft victim and a copy of my police report (or other investigative report or complaint to a law enforcement agency concerning identity theft) regarding identity theft is enclosed.

Yours Truly,

Your Name.

SAMPLE LETTER TO TRANSUNION – FOR PLACING A SECURITY FREEZE
(MUST BE SENT **CERTIFIED MAIL**)

Date

Trans Union Security Freeze
P.O. Box 6790
Fullerton, CA 92834-6790

Dear Trans Union:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one of the following:
I have included a $10 fee to place a security freeze on my credit file

OR

I am a senior (at least 65 years old) and the fee does not apply to me. OR

I am an identity theft victim and a copy of my police report (or other investigative report or complaint to a law enforcement agency concerning identity theft) regarding identity theft is enclosed.

Yours Truly,

Your name

SAMPLE LETTER TO EXPERIAN – FOR PLACING A SECURITY FREEZE
(MUST BE SENT **CERTIFIED MAIL**)

Date

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Dear Experian:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one of the following:
I have included a $10 fee to place a security freeze on my credit file

OR

I am a senior (at least 65 years old) and the fee does not apply to me. OR

I am an identity theft victim and a copy of my police report (or other investigative report or complaint to a law enforcement agency concerning identity theft) regarding identity theft is enclosed.

Yours Truly,

Your name

LOWRY HILL

RECOVERING FROM IDENTITY THEFT

1. ASSESS, DETERMINE AND PREPARE

   Assess the initial impact of the identity theft given what you know at the time the theft was first suspected. (For example, what type of personal data was lost? Which accounts seem to be the most at risk? etc.) Once you have assessed the situation, see if you can determine how the breach occurred. For example: "I discovered my computer had a virus last week, and I did some online banking the day before." Next, prepare to contact the various institutions that will help you contain and recover from the situation. When contacting each of the institutions, make sure you document to whom you spoke, when you spoke and the content of discussions. Similarly, make sure you save any correspondence and copies of any related documents.

2. PLACE A FRAUD ALERT WITH THE CREDIT BUREAUS

   Contact each of the credit bureaus, and have a Fraud Alert placed on your profile. While the bureaus claim that they share information, contacting each will ensure that you are protected sooner. To setup the alert, you will need to provide information, including your name, address, phone number, Social Security number, etc. Keep the alert active until, at a minimum, you have successfully worked with all of your financial institutions to ensure that your accounts have been adjusted accordingly.

   The three primary credit bureaus are:
   - Equifax: https://www.alerts.equifax.com
   - Experian: http://www.experian.com/fraud
   - TransUnion: http://www.transunion.com

   PLEASE NOTE THE FOLLOWING:
   - Your Fraud Alert may be required to be updated at least every 90 days
   - If you haven't received a confirmation from the credit bureaus stating that they have processed your Fraud Alert within two weeks of you initiating the alert, contact the respective credit bureau(s) again, and place the fraud alert once more.
   - While a Fraud Alert is in effect, it will create inconveniences related to opening new accounts.

3. CONTACT YOUR FINANCIAL INSTITUTIONS

   Contact the security/fraud departments of any institution at which you have a business relationship and explain your situation. Examples include, but may not be limited to banks, brokers and credit card companies.

4. FILE A COMPLAINT WITH THE FTC

   File a complaint with the FTC at https://www.ftccomplaintassistant.gov/ or by calling 1-877-IDTHEFT. Keep a copy for your records, as you may need it when communicating with some of the other institutions.

5. CONSIDER PLACING A CREDIT FREEZE WITH THE CREDIT BUREAUS

   A Credit Freeze is a stronger protective measure than a Fraud Alert because creditors and certain service providers are required by law (depending on the state) to review your credit report before processing a new service in your name. As of January 2009, 47 states had credit report laws on their books. These laws do vary from state to state, and the process for placing the Credit Freeze may be impacted by these laws. For example, you may be required to file a police report before you can establish a Credit Freeze. To get an understanding of your state's Credit Freeze laws, you can start by checking http://www.fightidentitytheft.com/credit-freeze-laws.html, contacting your state's Attorney General's office, or by directly contacting a credit bureau.

6. CONTACT OTHER POTENTIALLY IMPACTED INSTITUTIONS

   Contact the security/fraud departments of any other institution you feel may be impacted due to the situation. For example, if you are worried your insurance information may have been compromised, contact a representative at your insurance company/agency to see what can be done.

7. CHANGE YOUR IMPACTED SECURITY CREDENTIALS

If you in any way suspect that the credentials related to your digital life have been compromised, take the time to at least change the passwords to any service you think may be impacted. Before taking this step, make sure you are using a computer that is free from viruses, especially if you suspect that is the source of the breach. Examples of credentials you may need to change include, but are not limited to:

- Web-based e-mail (e.g., gmail, hotmail)
- Online banking and brokerage
- Social networking sites (e.g., FaceBook)
- Home security system PIN
- Credit card PINs
- eCommerce accounts (e.g., E-bay, Amazon, iTunes, NetFlix)

8. CONTACT YOUR IMMEDIATE FAMILY

At times, the situation may impact more than just an individual. The obvious example is when a spouse has his or her credit card number stolen, and that number is shared. In this situation, there is not only the potential to have a card denied at an inopportune time, but there may be the need to place a Fraud Alert or Credit Freeze on more than one Social Security number. Another more obscure example may be if an unsecured PDA was stolen and it contained information about a college-age child's address, phone number, SSN, etc. In these situations, it is better that all impacted parties be "in the know" (so everyone is acting in concert to prevent further damage).

9. CONTACT THE AUTHORITIES

- File an Identity Theft Report (or Fraud Report) with the police within 72 hours of first discovering the illegal activity. (Don't forget to keep a copy of the report for your records.)
- If the situation is related to Internet fraud, file a complaint with the FBI's Internet Crime Complaint Center at http://www.ic3.gov/default.aspx (and don't forget to keep a copy for your records).

10. REVIEW AND ADJUST

Review the situation, and assess if there is anything you can do to better protect yourself in the future. For example, you might consider maintaining a more secure computing environment by installing an updated security suite (e.g., Norton 360, McAfee Total Protection, or another reputable security suite), being more guarded about what you post online, adjusting how you track your credit information, etc.

11. MONITOR

Continue to monitor your situation for several months after you feel that the situation has concluded. For example:

- Pay closer attention to all financial statements (e.g., credit card statements, bank statements) for unexplained transactions.
- Pay closer attention to unusual messages associated with e-mail addresses used when purchasing online.

12. RESOURCES

- http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html
- http://www.fightidentitytheft.com
- http://www.idtheftcenter.org