A statewide group of legislators, law enforcements, prosecutors, business and financial industry security professionals, and private sector associations, working to reduce identity theft in Washington

January 27, 2012

Dear Business, Financial Institutions, Private Industry and Public Service Organization Leaders:

Over the last seven years, Washington State has made great gains to stop identity theft and financial fraud. Even with these gains, Washington remains in the top twenty states for complaints of financial fraud and identity theft. We are writing you on behalf of our organization, Law Enforcement Group against Identity Theft (LEGIT), to ask you to help make Washington State safe for you and our community.

LEGIT has worked hard over the past several years to strengthen the laws against identity theft:

- In 2005 we helped pass bipartisan legislation to strengthen data breach notification laws;
- In 2007 we proposed and passed legislation to enhance credit freeze requirements. Consumers can now freeze their accounts or be alerted when their credit history is requested, and not just after they have been victimized by identity theft;
- In 2008 we obtained passage of several laws to better protect identity theft victims. Victims can file police reports where they live, rather than in the multiple jurisdictions where their stolen identities may have been used. Identity thieves can also be punished for each time they use a victim's identity, rather than one conviction per victim, no matter how many times the crimes were committed with that identity;
- In 2009 we obtained passage of a bill that requires that only the last four digits of debit card numbers be printed on most retail receipts, supplementing the federal law that requires truncation of credit and debit card numbers on receipts and deletion of the expiration date; and
- In 2011 we achieved passage of legislation making the act of stealing mail and possessing stolen mail a felony. Previously it was only a misdemeanor.

Despite our legislative successes, we cannot reach our goal of crime reduction without your help. Identity thieves target businesses, government, and especially financial institutions to unlawfully obtain access to personal identifying information and the finances of consumers. Personal information includes, but is not limited to, these pieces of information:

- Name and address

- Telephone and cell phone number
- Driver's license or other government identification
- Place of employment
- Employee identification number
- Banking info – deposit account numbers, savings accounts, checking accounts
- Credit card number
- Passport number
- Alien registration number
- Health insurance number
- Taxpayer identification number
- School identification number
- PIN
- Computer or account passwords
- Email addresses
- IP addresses
- Date of birth
- Biometric data
- Birth certificate information
- Death certificate information
- Credit/loan applications

Criminals may use technology to hack into company databases, but they also employ low-tech methods such as stealing mail, dumpster diving, taking recycled materials or obtaining unencrypted computers. A significant amount of theft occurs from employees or vendors who have access to your records and databases. A current, alarming trend is the use of "skimming" devices placed over ATMs, gas pumps that take credit/debit cards, or other point-of-sale card readers. The skimming device collects account information off the magnetic strip on the back of the credit/debit card. Often, but not always, there is a pin-hole camera set up to obtain the PIN number associated with the debit card. This information is then transferred to a blank credit or debit card and used immediately to drain bank accounts and to rack up thousands of dollars in cash advances or credit card debt.

The goal of this letter is not to address all the areas of risk for you in your business operations. You likely already know of many risks and have taken steps to protect your customers. Rather, the purpose of this letter is to ask you to take the following risk reduction efforts, if you are not already, and to reinforce any current methods you have:

1. ***Destruction of Personal Identity Information.*** Federal and state laws require all businesses, banks, and other organizations ensure proper destruction of any sensitive consumer, financial, health or government identifiers contained in information received from consumers. These laws also require that when businesses retain this information, they must protect against unauthorized access to or improper use of sensitive consumer and financial information.

- What kind of personal identifying information is covered by these laws?
  Any record about an individual whether in paper, electronic, or any other form that is identifiable to an individual and is commonly used for financial or health purposes is subject to secure storage and destruction laws.

- What are reasonable data retention practices?

Scale down. Keep only consumer information that is required for business purposes or to meet legal obligations.

- What are reasonable destruction measures?
  Prior to destruction, the identifying information must be altered to the point where it cannot be read, deciphered, reconstructed or used by unauthorized persons. Shredding is an example of a way to destroy paper records. Wireless or electronic records may require different destruction methods.

- For information that is not destroyed due to business needs, what are reasonable storage measures?
  Electronic and Internet security is as important as the locks on your business doors. Are your computers and servers encrypted? Do you have effective policies regarding security of mobile devices? Is your software up to date to avoid Internet and software viruses? Do you restrict access to your information technology systems?

2. <u>What are key considerations in risk reduction?</u>

- Do you know what personal information about individuals you have in your files and on your computers?
- Do you keep only the information about individuals you need to conduct your business and comply with applicable laws?
- If you are a financial institution or other business that has accounts covered by the FTC's Red Flags Rule, do you have policies and procedures in place that can indicate the possible existence of identity theft and outline how to respond appropriately? (For more information about how to comply with this rule, see http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm .)
- Does your organization have written policies and procedures in place to assure proper disposal of personal information?
- Do you provide training to all staff on the policies? Can you demonstrate that you have provided training to each employee?
- Do you require your contractors to comply with the laws on destruction and breach of personal information?
- Do you require your contractors to comply with your policies?
- Have you established technical and physical safeguards to restrict access to personnel and files or other records containing personal information or other non-public identifying information regarding your own employees or consumers?
- Can you demonstrate that you limit access to both personal and non-public information to only those who actually need the information to allow employees to do their official duties?
- Do you perform security and background checks on all employees who have access to personal information and non-public information on consumers and employees?
- Do you truncate all personal numbers (social, telephone, accounts) on documents (paychecks, correspondence) with consumers and employees?
- What is your breach notification policy? Do you have trained staff to notify law enforcement, consumers, and other affected people if you experience a data breach?
- If you are a company with surveillance cameras, where are they placed? Are they at face level, which will maximize the ability for recognition? Are they in a place to capture the front of the face, as opposed to the side? Is the video of sufficient quality to be useful to law enforcement? The best placement tends to be on a door jamb where someone exits a location, about five feet from the ground. The quality should be at least 30 pixels between the eyes, which is a standard measurement for video quality.

- Are your credit card terminals safe from wireless hacking? Are you familiar with Payment Card Industry Rules (PCI)? Credit card companies have industry rules that require merchants to be audited if there is a breach in the credit card data, and the credit card companies levy steep fines if security is insufficient or eliminate a merchant's ability to use credit cards.
- Are your business computers safe from wireless hacking? If you have a wireless router, is the security setting WPA2? A security setting using an older level of security of WEP or WPA is vulnerable to hackers. Is the password for your security system a combination of symbols, numbers, uppercase letters and lower case letters? Is the password changed regularly?

Addressing each of these basic security concerns and implementing changes where appropriate can go a long way to protect your customers, your employees, and your organization from identity theft, fraud and abuse. The Attorney General's Office provides useful information on identity theft prevention specifically for businesses at www.atg.wa.gov. The King County Prosecuting Attorney's Office website at http://www.kingcounty.gov/Prosecutor.aspx has numerous helpful links if you are victim of a crime, including identity theft. The Federal Trade Commission is a great resource and provides helpful industry compliance information on its website at http://business.ftc.gov/privacy-and-security. Washington State Labor and Industries also has good information for identity theft victims at http://www.lni.wa.gov/ClaimsIns/CrimeVictims/default.asp. If you need legal advice on any of these issues, we suggest you confer with a private attorney who specializes in this area of practice.

We are pleased to count you among our partners in efforts to reduce identity theft crimes. Through our combined efforts, we can continue to make gains in our battle against fraud and identity theft. We seek to make our cities and counties the most hostile places in the nation to attempt to commit identity theft.

Sincerely,

ROB MCKENNA
Attorney General

DAN SATTERBERG
King County Prosecutor