DATA SECURITY

EVEN FOR A COUNTY/PUBLIC ENTITY – PROTECTING PERSONAL DATA IS REQUIRED

The theft of laptop computers storing personal information (including Social Security numbers) of 337,000 voters from election commission offices in Davidson County (Nashville, Tennessee) is a dramatic reminder that counties and other government agencies have a duty to protect the personal data they collect. Has your county/organization taken the appropriate measures to protect such personal data? This bulletin contains information created by the Federal Trade Commission on “Protecting Personal Information: A Guide for Business.”

WHY IS INFORMATION SECURITY IMPORTANT TO YOUR COUNTY’S OPERATION?

- According to Information Week, the amount of data captured and stored by businesses doubles every 12-18 months
- Failure to protect sensitive data can lead to identity theft or other harm to consumers – and can also harm your company
- Existing laws require many businesses to:
  - Implement reasonable and appropriate measures to protect sensitive consumer information
  - Notify consumers if there is a data breach
  - Protected information includes Social Security numbers, account information and information derived from credit reports

LEGAL STANDARDS

- Laws governing data security
  - Federal Trade Commission Act (FTCA)
  - Fair Credit Reporting Act (FCRA)
  - Gramm-Leach-Bliley Act (GLBA)
  - FTC Disposal Rule
  - Other federal laws (HIPAA, DPPA, FERPA)
  - State laws

The FTCA prohibits unfair or deceptive practices. To comply, you should:
- Handle consumer information in a manner consistent with your promises
- Avoid practices that create an unreasonable risk of harm to consumer data
- The FCRA requires consumer reporting agencies to “know their customers” and use “reasonable procedures” to allow access to consumer reports only to legitimate users
- The GLBA Safeguards Rule requires “financial institutions” to provide reasonable safeguards for customer data
- CAUTION! The definition of “financial institution” is broad, including auto dealers and courier services
- The Disposal Rule requires anyone who obtains a consumer report to use “reasonable” measures when disposing of it

*Content taken from: http://www.ftc.gov/bcp/edcams/infosecurity/slides.ppt
CREATING AN EFFECTIVE PLAN

A sound data security plan is built on five key principles, listed below. Our source material is from “Protecting Personal Information: A Guide for Business”, which can be found at www.ftc.gov/infosecurity.

1. Take stock
2. Scale down
3. Lock it
4. Pitch it
5. Plan ahead

1. TAKE STOCK. KNOW WHAT YOU HAVE AND WHO HAS ACCESS TO IT.
   - Check files and computers for:
     - What information you have
     - Where it is stored (don’t forget portable devices and offsite locations)
   - Trace the flow of data from entry to disposal, determining at every stage who has access – and who should have access

2. SCALE DOWN. KEEP ONLY WHAT YOU NEED FOR YOUR BUSINESS AND STREAMLINE STORAGE.
   - Collect only what you need, and keep it only for the time you need it
   - Scale down what you store on devices connected to the internet
   - Slip Showing? For receipts you give to customers, properly truncate credit card number and delete the expiration date
   - Limit the use of Social Security numbers
     - Social Security numbers can be used by identity thieves to commit fraud
     - Don’t collect Social Security numbers out of habit or convenience, but only when needed, such as to report wages to the government or to seek a credit report

3. LOCK IT. PROTECT THE INFORMATION YOU KEEP.
   - Training and oversight
     - Train your employees and overseas contractors and service providers
     - Use good hiring procedures and build information security training into orientation
     - Get handouts, tutorials, quizzes and tips at www.OnGuardOnline.gov
   - Computer security
     - Effective security covers data on your network and all devices, including laptops and PDAs
     - Remember the basics: firewalls, strong passwords, antivirus software

4. PITCH IT. PROPERLY DISPOSE OF WHAT YOU NO LONGER NEED
   - Shred, burn or pulverize paper records you don’t need
   - Use wipe utility programs on computers and portable storage devices
   - Place shredders around the office
   - If you use credit reports, you may be subject to the FTC’s Disposal Rule

5. PLAN AHEAD. CREATE A PLAN TO RESPOND TO SECURITY INCIDENTS AND BE READY TO HELP CONSUMERS.
   - Put together a “What if?” plan to detect and respond to a security incident
   - Designate a senior staff member to coordinate your response
   - Investigate right away and preserve evidence, such as computer logs
   - Take steps to close off vulnerabilities; e.g., disconnect compromised computers from the internet
   - Consider whom to notify if a breach occurs
   - If sensitive personal information is compromised, consumers may be at risk of identity theft
   - Plan to notify, as appropriate, law enforcement, other businesses and consumers
     - Remember: state law may require notice to consumers
   - Visit ftc.gov/infosecurity
ADDITIONAL TIPS

HELP CONSUMERS.
BE READY TO ASSIST
CONSUMERS WHO ARE
VICTIMS OF FRAUD.

- Under the FCRA, a business must:
  - Provide consumers with certain information about a fraud
  - Verify the identity of any applicants who have fraud alerts on their credit report files
- Under the FCRA, under certain conditions, a business may not:
  - Sell or collect on a fraudulent debt
  - Report a fraudulent debt to the credit bureaus

MORE HELP FOR CONSUMERS. WE ALSO SUGGEST THAT YOU:

- Give victims information about how to recover from identity theft and refer them to FTC for more help: www.ftc.gov/idtheft or 877-ID-THEFT
- Give them information on the documents you will require from them to resolve fraudulent debts
- Give them closure letters absolving them of fraudulent debts once an incident is resolved

CONTACT INFORMATION

For additional information, please contact:

Bob Lombard
Sr. Vice President & Regional Director
Willis Pooling Practice
1755 E. Plumb Lane, Suite #269
Reno, NV 89502
775 323 1656 Ext. 19 (Office)
775 858 6335 (Cell)
lombard_bj@willis.com