



**FOR IMMEDIATE RELEASE**

September 27, 2006

**BEST PRACTICES FOR BUSINESSES, BANKS, AND HEALTH CARE PROVIDERS TO  
SAFEGUARD PERSONAL IDENTIFYING INFORMATION  
AND FIGHT IDENTITY THEFT**

**All Businesses, Banks, and Health Care Providers:**

- \* Limit physical access to business and human resources computers and files with personal identifying and bank account information to those who need access. Use automatic log-off software.
- \* Secure access to personal identifying information especially at night. Keep surveillance cameras operating 24/7.
- \* Mandate security and background checks on employees handling personal identifying information.
- \* Train employees to follow secure practices with personal identifying information, and monitor their adherence.
- \* Have log-on software so you know who is accessing personal identifying information in business and human resources computers.
- \* Consider procedures for dual control and for safeguarding passwords when appropriate.
- \* Review use of social security numbers in your business. Consider steps to restrict, eliminate, or conceal their use, substituting unique user names and pin #s.
- \* Use encryption software and software that detects malicious programs when appropriate.
- \* Impose requirements for the adequate disposal (shredding, erasing) of personal identifying information that will no longer be retained.

- \* Adopt procedures for notifying customers of breaches of security with regards to personal identifying information.
- \* Use diligence in selecting and monitoring agents, contractors and service providers, (e.g. janitorial services) Require that such entities follow similar precautions with personal identifying information received from you.
- \* Periodically test key controls, and review security of personal identifying information in light of changes in technology, personnel, sensitivity of customer information, and security threats.
- \* Appropriately sanction employees who violate security policies. End access to personal identifying information by terminated employees.

**Banks/Financial Institutions in Particular:**

- \* Ensure that employees ask for IDs when conducting transactions.
- \* Train employees in fraudulent document recognition and to recognize security features.
- \* Capture digital images of identity source documents, i.e. driver's license photos, when account is opened. Ideal system: Photo identification comes up on screen at teller window during transaction.
- \* Either require that customers set up online banking in person with ID or have customer choose unique name and password at the time the account is opened that must be provided when online banking is initiated.
- \* Notify account holder in writing by U.S. mail when online banking is initiated.
- \* Take thumb prints and/or index fingers for cashing "on us" checks.
- \* Use special equipment to check IDs for security features.
- \* Train tellers to give additional scrutiny to out-of-state IDs used on long established accounts.
- \* Improve the quality of video/photo surveillance, especially at teller windows (full frontal view) and drive up windows.
- \* Keep the video tapes for longer periods of time (at least 90 days).

- \* Record, and keep for a reasonable period of time, all incoming customer service calls.
- \* Ensure that employees who receive incoming customer service calls (change of address, online banking) do not deviate from information required to access accounts -- regardless of the story the caller tells. Train employees to ask better questions, and require that certain fields of authenticating information be obtained. Require information that is not on the bank statement.
- \* When customers make a change of address on an account, send written confirmation to both the new and the old addresses.

### **Some State and Federal Laws and Regulations Governing Data Security**

- \* Title 12 C.F.R. Parts 30, 208, 225, 364 and 570 – Guidelines Establishing Information Security Standards for Banks and Financial Institutions
- \* Title 16 C.F.R. Part 682 – Proper Disposal of Consumer Information under the Fair Credit Reporting Act
- \* Title 17 C.F.R. Part 248 (Regulation S-P) -- Procedures to Safeguard Customer Records and Information For Brokers, Dealers and Investment Companies
- \* Title 45 C.F.R. Parts 160, 162, 164, 403 – Privacy, Security, Administrative Data Standards under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- \* Revised Code of Washington Chapter 19.215 – Removal and Disposal of Personal Information by Commercial, Governmental, and Other Entities
- \* Revised Code of Washington Section 42.56.590 – Personal Information – Notice of Security Breaches