W. A. DREW EDMONDSON
ATTORNEY GENERAL OF OKLAHOMA

MEMORANDUM

TO: All State Agencies

FROM: W. A. DREW EDMONDSON
ATTORNEY GENERAL

DATE: May 6, 2009

SUBJECT: "Breach of the security of the system"

Oklahoma media has reported on several recent events where a state agency has misplaced, lost or reported as stolen the personally identifiable information of residents of the State of Oklahoma. As hard as we try to keep this critical information safe, sometimes the worst happens, and sensitive personal information is compromised. Oklahoma statutes have set out certain steps agencies of state government must follow in the event of a security breach. The purpose of this letter is to inform you of these legal requirements in the event that a breach occurs at your agency.

A security breach, otherwise known under Oklahoma Statutes as a "breach of the security of the system," occurs when an unauthorized acquisition of computerized data compromises the security, confidentiality or integrity of personal information.

When these incidents occur, the state agency, according to 74 O.S. Supp. 2008, §3113.1, is under the obligation to notify residents without unreasonable delay, consistent with the legitimate needs of law enforcement. State agencies have the duty to inform residents by a written notice or by email as mandated by Section 7001 of Title 15 of the United States Code. If a written notice is not possible due to the cost exceeding $250,000.00 or the residents affected exceeds 500,000 or the agency does not have enough information, then the agency can use substitute methods of notification. The agency can use email, conspicuously post the notice on the agency's website or notify residents through statewide media.

I would urge state agencies to combine the variety of methods above to ensure that residents will receive notice. Additionally, you may want to provide the following information to help those affected by the breach protect themselves from fraud and identity theft.

313 N.E. 21ST STREET • OKLAHOMA CITY, OK 73105-4894 • (405) 521-3921 • FAX: (405) 521-6246

recycled paper

Affected residents should:

Consider placing an initial fraud alert in your file at all three major credit reporting bureaus.
Equifax: (800) 525-6285
Experian: (888) 397-3742
TransUnion: (800) 680-7289

Request a free copy of your credit reports and dispute any errors or unauthorized use. You are entitled to receive a free credit report every year from all three credit reporting bureaus. Reports may be requested by phone at (877) 322-8228, by mail at Annual Credit Report Request Service, PO Box 105281, Atlanta, GA, 30348-5281 or online at www.annualcreditreport.com. You may want to wait about one month to request the credit report because suspicious activity may not show up right away.

Notify all financial institutions, including banks, credit unions and credit card companies of the potential for fraud.

Monitor monthly financial statements closely and dispute any unauthorized charges.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission.

Currently, there is no standard set forth in the Oklahoma Statutes for protecting the security, confidentiality or integrity of personal information. However, the following guidelines should be considered by state agencies.

1. Does the agency really need to collect and store personal information such as social security numbers, credit and debit card numbers and dates of birth? Is it strictly necessary to accomplish the business purpose or mission? Is there another way to identify residents?

2. Limit the number of personnel that have access to personal information.

3. Require appropriate training of personnel that have access to the information.

4. Consider prohibiting or strictly limiting access to personal information from portable devices such as laptops, personal digital assistants or cell phones.

5. Restrict the ability to duplicate or copy the information on portable devices such as thumb

drives and flash drives to key personnel such as administrators or chief information officers.

6. Encrypt all portable and storage devices that store personal information. Especially encrypt devices such as laptops and storage drives that might be moved to another location.

7. Coordinate with privacy officers, chief information officers and legal counsel to develop the appropriate steps that should be implemented within your agency.

8. Continue to remain vigilant with new employees and equipment.

We live in a fascinating time where advances in science and technology are rapidly changing the way we conduct business; computers have replaced typewriters and file cabinets have given way to thumb drives. One thing that has not changed is our duty to protect the personal information of the residents we serve. As public servants, we are required by law to inform residents when this information may be compromised, and I believe we also have the obligation to arm them with useful information so they can protect themselves from fraud and identity theft.

Thank you for your attention to this important issue and for the service you provide to the people of our state.