**The Office of Government Ethics' policy on Breach of Personally Identifiable Information provided below is under review. The policy is under review and may be revised. If you require additional information, please contact us. (See the *Contact OGE* section of this web site for information on how to contact OGE via mail, email, or phone.)**

# BREACH OF PERSONALLY IDENTIFIABLE INFORMATION

## Background

Safeguarding personally identifiable information (name, date of birth, social security number, etc.) is a responsibility shared by all OGE employees and contractors. As such, safeguarding personally identifiable information in the possession of the OGE and preventing the breach of that information is essential to ensuring the trust of individuals working with OGE as well as the trust of its employees, contractors and the general public. To help safeguard personally identifiable information, OGE will comply with the requirements of all applicable laws and regulations, including the Federal Information Security Management Act (FISMA) and related policies and guidance from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

A breach of personally identifiable information may result in harm to an individual on whom information is maintained. Such harm may include the effect of a breach of confidentiality, the potential for blackmail, emotional distress, or unwarranted exposure leading to humiliation or loss of self-esteem. A breach of personally identifiable information can result in identity theft, a situation in which individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes. Identity thieves can use financial account identifiers, such as credit card bank account numbers, to commandeer an individual's existing accounts to make unauthorized charges or withdraw money. Thieves can also use accepted identifiers like social security numbers to open new financial accounts and incur charges and credit in an individual's name without the that person's knowledge.

## Core Response Group

Upon the identification of a potential loss of personal information, a group consisting of OGE's General Counsel, Privacy Officer, Chief Information Officer, Records Officer, and the senior management official of the office responsible for the record(s) in question will evaluate the situation and guide any further response. Actions by the response group may vary depending on the circumstances of each particular situation. Because of those varying circumstances, the response group may seek the expertise of other OGE officials and law enforcement organizations. In addition to considering the data that was compromised, the response group will also consider the following:

- how easy or difficult it would be for an unauthorized person to access the information in light of the manner in which the information was protected (i.e. information on a stolen laptop computer);
- the means by which the loss occurred, including whether the incident might be the result of criminal activity or likely to result in criminal activity;
- the ability of the Agency to mitigate the identify theft;
- evidence that the compromised information is actually being used to commit identity theft;
- notifying the issuing bank , if the breach involves a government authorized credit card; and
- if the breach involves employees' bank account numbers used for the direct deposit of reimbursements and salaries or benefit payments, the bank or organization handling those transactions should be notified.

Before making a breach notification, the response group should address the following six factors:

- Whether Breach Notification is Required
- The Timeliness of the Notification
- The Source of the Notification
- The Contents of the Notification
- The Means of Providing the Notification (mail, telephone, website, etc)
- Who Receives the Notification: Public, Agency employees, etc.

Should the response group decide to provide a notice to those put at risk, the notification should be timely without compounding the harm through a premature announcement based upon incomplete facts or in a manner likely to make identity theft more likely to occur. The notice should include the following elements:

- a brief description of what happened;
- to the extent possible, a description of the types of personal information that were involved in the data breach (e.g. full name, social security number, date of birth, home address, account number, etc.);
- a statement as to whether the information was encrypted or protected by other means when it is determined that such information would be beneficial and would not compromise the security of the records system;
- a brief description of what the Agency is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
- contact information for those employees wishing to learn additional information; and
- the steps individuals should take to protect themselves from the risk of identity theft (see below).

As soon as possible after the discovery of a breach and the decision to provide notification to the public, the Agency should post information about the breach and notification prominently on the OGE web site. The posting should, as appropriate, include a link to Frequently Asked Questions and other talking points to assist the public's understanding of the breach and notification process. The information should also appear on the www.USA.gov web site.

Actions by Employees

The steps that individuals can take to protect themselves depend on the type of information that has been compromised. Employees should focus on steps that are relevant to their particular circumstances and applicable with state law concerning usability and costs. Such steps may include the following:

- Contact their financial institution to determine whether their account(s) should be closed.
- Monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. Consumers are entitled by law to obtain one free credit report per year from each of the three major credit bureaus (Equifax, Experian, and TransUnion) for a total of three reports every year. The annual report can be used as a self monitoring tool as well as a way to check credit without initiating a fraud alert;.
- Place a fraud alert on the credit reports maintained by the three major credit bureaus. This option is most useful when the breach includes information that can be used to open new accounts, such as social security numbers. The alert signals credit issuers who obtain credit reports that they should take steps to verify the consumer's identity before issuing credit.
- Placing a credit freeze on their credit file. Doing so precludes third party access to a consumer's credit report, thereby effectively preventing the issuance of new credit in the consumer's name.
- Review resources provided on the Federal Trade Commission (FTC) identity theft website at www.ftc.gov/idtheft .
- Be aware that the public announcement of the breach could itself cause criminals, under the guise of providing legitimate assistance, to use various techniques, including the telephone and email, to deceive the individuals affected by the breach into disclosing their credit card numbers, bank account information, social security numbers, or other personal information. One common such technique is "phishing," a scam involving an email that appears to come from a bank or other organization that asks the individual to verify account information, and then directs the individual to a fake website whose only purpose is to trick the individual into divulging his/her personal information. See FTC's web site at

http://www.ftc.gov/bep/edu/pubs/consumer/alerts/alt166.htm for information on this type of fraud.

Rules and Consequences

Consequences of a data breach should be commensurate with the type of personal identifiable information involved. Individuals shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

- Fail to implement and maintain security controls, for which they are responsible and aware, for personally identifiable information regardless of whether such action results in the loss of control or unauthorized disclosure of personally identifiable information;
- Exceed authorized access to, or disclose to unauthorized persons, personally identifiable information;
- Fail to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information; and
- For managers, fail to adequately instruct, train, or supervise employees in their responsibilities.

Sanctions could include reprimand, suspension, removal, or other actions in accordance with applicable law and Agency policy. At a minimum, the access authority of any individual demonstrating reckless disregard or a pattern of error in safeguarding personally identifiable information should be removed.