U.S. Department of Justice

Incident Response Procedures for Data Breaches Involving Personally Identifiable Information

Version 1.6 August 7, 2008

Table of Contents

PREFACE

On September 20, 2006, the Office of Management and Budget (OMB) issued a Memorandum to the leadership of the Departments and Agencies entitled "Recommendations for Identity Theft Related Data Breach Notification." The memorandum provides recommendations for planning for and responding to data breaches and losses involving personally identifiable information (PII). Among the recommendations is the establishment of a core management team in each Department responsible for responding to the loss of personally identifiable information. In addition, OMB Memorandum 07-16, dated May 22, 2007, entitled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" requires agencies to develop and implement a notification policy for breach of PII.

The following procedures address the recommendations and their implementation within the Department of Justice (DOJ).

Record of Changes

Revisions to this document will be issued periodically to reflect changes to policy, procedures, or responsibilities that do not warrant an update to the entire document. Changes will be issued by replacing entire Chapters, Sections, or pages. A complete list of all revisions will be issued with each new change to ensure all documents are kept current. Changes should be entered in the document and recorded in the Table below.

Change Number	Date of Change	Section	Description of Change	Change Entered By
Version 1.0	Feb. 2007	Full Document	Initial Draft	Kevin Cox
Version 1.1	Feb 23, 2007	Full Document	Described applicability, expanded list of definitions, included contractor-managed systems for DOJ, added language regarding Component involvement, and added mitigation steps for addressing risk of physical or financial harm	William Pailen
Version 1.2	Mar 21, 2007	5.0, 9.0, and 12.0	Added Figures 1, 2, and 3	William Pailen
Version 1.3	Mar 28, 2007	Full Document	Removed emphasis on identity theft, removed Acknowledgements Section, and removed some acronyms and figures	Kevin Cox
Version 1.4	April 2, 2007	Full Document	Removed 'Limited Official Use' header and footer, revised definitions, adding clarifying wording, and modified Figure 2.	Kevin Cox
Version 1.5	August 10, 2007	Full Document	Updated to reflect Component Comments and cross referenced document to OMB Memorandum 07-16	Kevin Deeley
Version 1.6	March 7, 2008	Full Document	Updated to more clearly reflect contractor responsibilities and clarify certain terms	Niels Quist

1.0 PURPOSE

In its September 20, 2006, memorandum addressing identity theft related data breach notification, OMB writes, "Given the volume of personal information appropriately collected to carry out myriad government functions, it is almost inevitable that some agencies will, on occasion, lose control of such information." Agencies must be prepared for such losses and should respond accordingly to protect the individuals who might be affected. The purpose of this document is to set forth the DOJ's plan for responding to data breaches involving PII, should they occur within any of its Components or in connection with work done by its contractors. It addresses the detection and reporting of such incidents, the assessment of their risk, the proper escalation to upper-level management, and the appropriate notification and remedy options.

2.0 SCOPE

These procedures provide mitigation strategies and responses to intentional or inadvertent data breaches involving PII in the control of the DOJ or contractors who process, store, or possess DOJ PII. It includes procedures for organizational actions in response to such events.

3.0 APPLICABILITY

The provisions and guidelines of these procedures apply to any data breach involving PII, as defined in these procedures. The procedures were developed with the intent of maintaining a balance between data breach notification to affected individuals and protection of the integrity of law enforcement and national security cases and investigations. General data breach procedures are located in the DOJ IT Security Standard for Incident Response (IR) and the IR Plan (IRP) Template issued by the DOJ Computer Emergency Readiness Team (DOJCERT). For a description of computer security incidents, refer to NIST Special Publication 800-61, *Computer Security Incident Handling Guide.* In addition to the general data breach procedures to be followed whenever there is a breach of any kind of Department data, these DOJ Incident Response Procedures for Data Breaches Involving Personally Identifiable Information (previously entitled Data Breach Notification Procedures) provide procedural requirements for data breaches that involve PII.

The provisions and guidelines of these procedures apply to, and define the responsibilities of, the following:

- DOJ Core Management Team
- DOJCERT
- All DOJ personnel, contractors, and others who process, store, or possess PII on behalf of DOJ

4.0 DEFINITIONS

Component – Includes all bureaus, offices, boards, and divisions of the Department of Justice.

Data Breach – Includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, access for an unauthorized purpose, or other unauthorized access, to data, whether physical or electronic.

Personally Identifiable Information (PII) –

Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

Information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006.

The above definitions have been developed by OMB. Please note that the items listed in those definitions are meant to serve as examples and do not represent a comprehensive list of personally identifiable information.

Information that standing alone is **not generally considered personally identifiable**, because many people share the same trait, includes:

- First or last name, if common (For example: Smith or Brown)
- Country, state, or city of residence
- Age, especially if non-specific (such as age in years, without birthdate)
- Gender or race
- Workplace or school
- Grades, salary, or job position

Sometimes multiple pieces of information, none of which alone may be considered personally identifiable, may uniquely identify a person when brought together.

Identity Theft – The act of obtaining an individual's identifying information without authorization in an attempt to commit or facilitate the commission of fraud or other crimes. The resulting crimes usually occur in one of the following ways. Identity thieves may attempt to:

- Gain unauthorized access to existing bank, investment, or credit accounts using information associated with the individual.
- Withdraw or borrow money from existing accounts or charge purchases to the accounts
- Open new accounts with an individual's personally identifiable information without that individual's knowledge
- Obtain driver's licenses, social security cards, passports, or other identification documents using the stolen identity

5.0 LIMITATIONS

A. Notification to individuals affected by a data breach involving PII may not occur or may be delayed if a national security or law enforcement agency determines that the notification will impede a law enforcement investigation or jeopardize national security. This determination will be made by the Core Management Team after consultation with the cognizant law enforcement agency.

B. In cases where a contractor processes, stores, possesses, or otherwise handles the PII that is the subject of a data breach, any notification to individuals affected by the data breach must be coordinated with the Department. No notification by the contractor may proceed until the Department has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by the contractor must be coordinated with, and is subject to the approval of, the Department.

6.0 DOJ CORE MANAGEMENT TEAM

The organizational backbone for the DOJ response to an actual or suspected data breach involving PII is the DOJ Core Management Team. The Core Management Team convenes in the event of a significant data breach involving personally identifiable information. The Core Management Team engages in a risk analysis to:

- Determine the extent to which the breach poses problems related to identity theft
- Manage activities to recover from the breach and mitigate the resulting damage

The DOJ Core Management Team consists of the following officials:

- Office of Attorney General
- Principal Associate Deputy Attorney General
- Associate Attorney General
- Assistant Attorney General, Office of Legal Counsel
- Assistant Attorney General, Office of Legislative Affairs

- Assistant Attorney General, Administration
- Associate Deputy Attorney General, permanent
- Chief Information Officer
- Chief Privacy and Civil Liberties Officer
- Inspector General
- Director, Office of Public Affairs
- Program Manager and Senior Component Official for Privacy, Executive Officer, or other legal counsel from component experiencing breach

The DOJ Core Management Team is chaired by the Chief Information Officer and Chief Privacy and Civil Liberties Officer and is supported by the staff members of each of the offices represented.

The DOJ Core Management Team should convene at least annually to review these procedures and discuss likely actions should an incident occur.

7.0 RISK-BASED DECISION FRAMEWORK

A data breach involving PII, may, but need not necessarily, present a significant risk of harm. For example, a data report showing "John Smith," with little or no further identifying information related to John Smith, will, in many circumstances, present little or no risk of harm resulting from the exposure of the information. On the other hand, release of the identity of a person in a witness protection program may jeopardize the safety of the person identified. Thus, the first steps in considering whether there is a risk, and hence whether a response is necessary, are understanding the kind of information most typically used to personally identify a specific individual and then determining whether that kind of information has been or potentially was compromised in the incident being examined. Because circumstances will differ from case to case, the DOJ should draw upon law enforcement expertise in assessing the risk of the breach of PII and the likelihood that the incident is the result of or could lead to criminal activity.

A SSN standing alone can identify an individual and lead to identity theft. Combinations of information can have the same effect. With a name, address, or telephone number, identity theft becomes possible, in combination with any of the following: (1) any government-issued identification number (such as a driver's license number if the thief cannot obtain the SSN); (2) a biometric record; (3) a financial account number, together with a PIN or security code; or (4) any additional, specific factor that adds to the personally identifying profile of a specific individual, such as a relationship with a specific financial institution or membership in a club.

Figure 1 provides a model that can be used as guidance for analyzing the risk associated with exposure of PII. However, each incident may have unique risk factors. Therefore, the method of risk analysis for each incident must be based upon the circumstances surrounding that incident.

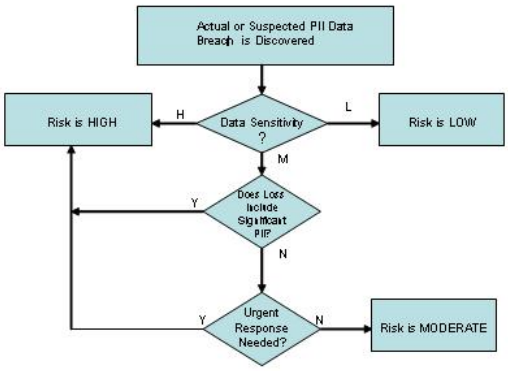

Fig. 1 – Assessing PII Risk

Factors to Consider in Determining Urgency

- Effectiveness of Security Technologies (Strong, Weak) - for example, encryption or no encryption on a laptop
- Likelihood Data is Usable (High, Low)
- Data Sensitivity (High, Moderate, Low)
- Data Volume (i.e., amt. of data lost) (High, Low)
- Likelihood Data Loss Can Cause Harm (High, Low)
- Was the Data Intentionally Targeted (Yes, No)

Considering these factors together should permit the DOJ to develop an overall sense of the risk of harm associated with a particular incident. That assessment should then guide the DOJ's further actions.

The following sections outline the stages associated with the risk assessment process of a data breach involving PII. Risk assessment occurs throughout the process.

8.0 STAGE 1: INCIDENT DETECTION AND REPORTING

A. Actual or Suspected data breaches must be reported to the DOJCERT immediately.

1. Other Component Requirements

Component Management should be notified of the PII incident within their Component and support the investigation, mitigation, and recovery activities of the DOJ Core Management Team. The following Component personnel should be notified of the incident. These individuals should meet, as appropriate.

- Component Head or designee
- Component Chief Information Officer

- Senior Component Official for Privacy, Executive Officer, or other Legal Affairs Representative
- Component Security Program Manager
- Incident response team representative
- Owner or manager of the system from which the loss occurred

2. Other Contractor Requirements

Contractors shall notify the Contracting Officer (CO), and the Contracting Officer's Technical Representative (COTR) immediately (and in all cases within one hour of discovery) of any data breach. If the data breach occurs outside of regular business hours and/or neither the CO nor the COTR can be reached, the contractor shall contact DOJCERT. Contractors shall cooperate with all aspects of DOJ's investigation, assessment, mitigation, and recovery activities.

B. DOJCERT will analyze all incidents and will work with the reporting Component to record the incident information into the DOJCERT Database. Within the DOJCERT Database, the affected Component performs an assessment of the risk to the DOJ and to the individuals whose PII is compromised at the time of incident. The assessment takes into account the following.

- Sensitivity of the Data Lost[1]
- Amount of Data Lost and Number of Individuals Affected
- Likelihood Data Is Usable or May Cause Harm
- Likelihood the Data Was Intentionally Targeted
- Strength and Effectiveness of Security Technologies Protecting Data
- Nature of the Data: Operational or Personal
- Ability of the Agency and/or Contractor to Mitigate the Risk of Harm

The DOJCERT Staff also performs their own assessment based on the details included with the incident report. The risk levels are High, Medium, or Low.

C. DOJCERT will notify US-CERT within the OMB-mandated one hour timeframe and will start the internal alerting and notification process.

9.0 STAGE 2: INTERNAL ALERTING AND RISK ASSESSMENT

[1] *As stated by OMB in Memorandum 07-16, sensitivity of data elements is contextual. For example, a breach of a database containing names of individuals being investigated for tax fraud may pose a higher risk of harm than a database of names of persons who subscribe to an agency newsletter.*

A. For incidents with a risk rating of either Medium or High, DOJCERT will send an e-mail notification to the Office of Privacy and Civil Liberties, the Office of the Inspector General (OIG), the Office of the Chief Information Officer (OCIO), the Security and Emergency Planning Staff, and the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division.

B. The e-mail shall contain the known details of the incident, as well as the actions that have been taken to respond to it thus far. It also includes an initial risk rating.

10.0 STAGE 3: ESCALATION

A. After initial notification, DOJCERT will perform a more thorough analysis of the incident. As above, the analysis will consider the following.

- Sensitivity of the Data Lost
- Amount of Data Lost and Number of Individuals Affected
- Likelihood Data Is Usable or May Cause Harm
- Likelihood the Data Was Intentionally Targeted
- Strength and Effectiveness of Security Technologies Protecting Data
- Nature of the Data: Operational or Personal
- Ability of the Agency and/or Contractor to Mitigate the Risk of Harm

Following the analysis, DOJCERT will prepare a Summary of Facts with Recommendations for the CIO and CPCLO. The CIO and CPCLO will then notify the DOJ Core Management Team. If the risk is high, the Deputy Attorney General will also be notified and will convene the DOJ Core Management Team.

B. DOJCERT will also work with the Criminal Division, Computer Crime and Intellectual Property Section (CCIPS) to determine whether further investigation is required by law enforcement. As appropriate, CCIPS will notify the Federal Bureau of Investigation (FBI).

C. Figure 2 illustrates the overall processes involved in reporting, handling, and escalating an incident.

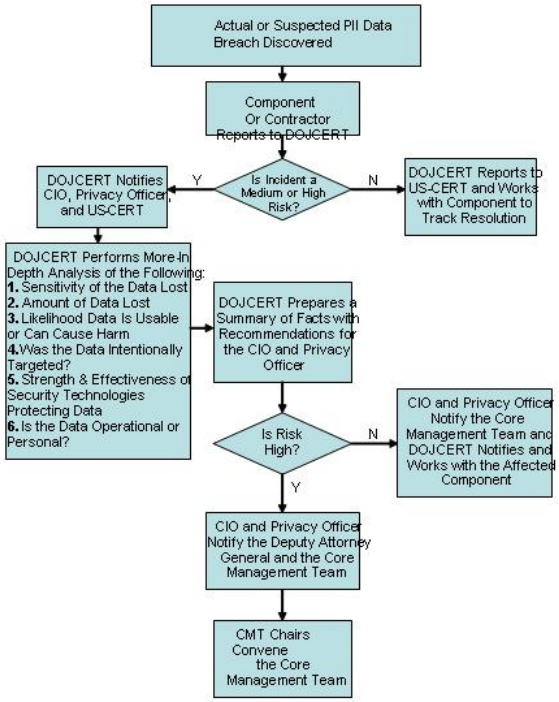

Fig. 2 – Handling PII Loss

11.0 STAGE 4: ASSESSMENT AND MITIGATION

A. The DOJ Core Management Team will assess the details of the incident and will determine the appropriate course of action, including the level of notification required to affected individuals, the resources needed, and any appropriate remedy options. The Core Management Team will also need to determine whether Congress should be notified.

B. The DOJ Core Management Team should simultaneously consider options for mitigating the risk. The following two sections detail the standard options available to agencies and individuals to help protect potential victims.

C. Actions that Can Be Taken for Mitigating the Risk

The actions below can be taken by DOJ or a contractor who was involved in a data breach involving PII. Contractor responsibilities shall be addressed in the contract.

- If the breach involves individuals' banking, credit card, or other financial PII, DOJ or the contractor should notify the individuals and inform them of steps that they should take to mitigate the risk. Written notification procedures are contained in Appendix A. Where necessary, the Department or contractor should assist the individuals' mitigation efforts.
- If the breach involves a large volume of users, DOJ or the contractor should consider establishing a Help Line that allows affected users to call in to DOJ or the contractor to learn information. Appendix B contains more information regarding the procedures for establishing a Help Line.
- If the breach of PII has the potential to compromise the physical safety of the individuals involved, DOJ should ensure that the appropriate law enforcement agencies are notified and that the agencies take appropriate protective action.
- If the breach involves government-authorized credit cards (such as a loss of a card or card number), DOJ should notify the issuing bank promptly. If the breach involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit payment, DOJ should notify the bank or other entity that handles that particular transaction for the agency.
- DOJ or the contractor may take two other significant steps that can offer additional measures of protection but which will involve agency or contractor expense. They are:
    - Data Breach Analysis – Using new technology, analyze whether a particular data loss appears to be resulting in identity theft. DOJ or the contractor may consider using this measure if it is uncertain about whether the identity-theft risk warrants implementing more costly additional steps or if it wishes to do more than rely on individual actions.
    - Credit Monitoring – In deciding whether to offer credit monitoring services and of what type and length, DOJ should consider the seriousness of the risk of identity theft arising from the data breach involving PII. Particularly important are whether identity theft incidents have already been detected and the cost of the service. To assist the timely implementation of either data breach analysis or credit monitoring, the General Services Administration (GSA) is putting in place several government-wide contracting methods to provide these services if needed. If a contractor is responsible for the data breach involving PII, the contractor may provide credit monitoring and/or other corrective action in coordination with the Department.

D. Actions that Individuals Can Routinely Take for Mitigating the Risk

- Contact their financial institution to determine whether their account(s) should be monitored or closed. This option is relevant only when financial account information is part of the breach.

- 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. It may take a few months for most signs of fraudulent account activity to appear on the credit report. This option is most useful when the data breach involves information that can be used to open new accounts.
- Contact the three major credit bureaus and place an initial fraud alert on credit reports maintained by each of the credit bureaus. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs.
- For residents of states in which state law authorizes a credit freeze, consider placing a credit freeze on their credit file. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs.
- For deployed members of the military, consider placing an active duty alert on their credit file. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs.
- Review resources provided on the Federal Trade Commission (FTC) identity theft Website, www.ftc.gov/idtheft.
- Complete a Federal Trade Commission ID Threat Affidavit at the above FTC Website. This will allow an individual to legally notify their creditors that their identity has been compromised. Any debts incurred after that date will not be assigned to them.
- Be aware that the public announcement of the breach could itself cause criminals engaged in fraud to use various techniques to deceive individuals affected by the breach into disclosing their personal information.

12.0 STAGE 5: NOTIFICATION TO AFFECTED INDIVIDUALS, RECOVERY, AND RESOLUTION

Having identified the level of risk and bearing in mind the steps that can be taken by the DOJ to limit that risk, the DOJ should then move to implement a corrective action plan. The Core Management Team should bear in mind that notice and the response it can generate from individuals is not "costless," a consideration that can be especially important where the risk is low. The costs can include the financial expense and inconvenience that can arise from canceling credit cards, closing bank accounts, placing fraud alerts on credit files, and/or obtaining new identity documents. Moreover, frequent public notices of such incidents may be counterproductive, making it more difficult for citizens to discern the difference between serious and minor threats. Thus, weighing all the facts available, the risks to citizens caused by the data breach warrant a notice when a notice would facilitate appropriate remedial action that is justified given the risk.

Assuming the DOJ Core Management Team has made the decision to provide notice to those put at risk, the following elements should be incorporated into the notification process.

A. Timing

The notice should be provided in a timely manner, but without compounding the harm from the initial incident through premature announcement based on incomplete facts or in a manner likely to make identity theft more likely to occur as a result of the announcement. In addition, sometimes an investigation of the incident can be impeded if information is made public prematurely. Any notification or delay of notification should be coordinated with the cognizant law enforcement agency conducting the investigation of the breach.

B. Source

Given the serious security and privacy concerns raised by data breaches, notification to individuals affected by the data loss should be issued by a responsible official of the DOJ, or, in those instances in which the breach involves a publicly known Component, a responsible official of the Component.

When the breach involves a contractor, the source of the notice may appropriately come from the contractor. In general, to avoid creating confusion and anxiety, the notification should come from the entity which the affected individuals are reasonably likely to perceive as the entity with which they have a relationship. But in all cases, notification by a contractor must be coordinated with DOJ.

1. Contents

The substance of the notice should be reduced to a stand-alone document and written in clear, concise, and easy-to-understand language, capable of individual distribution and/or posting on the DOJ Website and other information sites (See Appendix A). 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 security breach (e.g., full name, SSN, date of birth, home address, account numbers, disability code, etc.);
- a brief description of what the agency is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
- contact procedures for those wishing to ask questions or learn additional information, including a toll-free telephone number, Website, and/or postal address; and
- steps individuals should take to protect themselves from the risk of identity theft.

Any specific PII affected by the data breach is sensitive and should be treated as such. It should not be e-mailed over the Internet unencrypted and should be wrapped appropriately when hand-carried.

Given the amount of information needed to give meaningful notice, DOJ may want to consider providing the most important information up front, with the additional details in a set of Frequently Asked Questions (FAQ) format on its Website. If DOJ has knowledge that the affected individuals are not English speaking, notice should also be provided in the appropriate language(s).

2. Method of Notification

Notification should occur in a manner calibrated to ensure that the individuals affected receive actual notice of the incident and the steps they should take. According to OMB, first-class mail notification to the last known mailing address of the individual should be the primary means by which the agency provides notification.

Substitute means of notice such as broad public announcement through the media, Website announcements, and distribution to public service and other membership organizations likely to have access to the affected individuals, should be employed to supplement direct mail notification or if the DOJ cannot obtain a valid mailing address. Media notification should focus on providing information to aid the public in our response to the breach.[2]

E-mail notification can be problematic and is discouraged unless the affected individuals consent to such use.[3] Care should be made not to solicit information from affected individuals as they could encounter difficulties in distinguishing the agency's e-mail from a phishing e-mail. If there is an ongoing criminal investigation, notification under these provisions should be coordinated with DOJ Victim notification procedures under the Automated Victim Notification System.

DOJ should also give special consideration in providing notice to individuals who are visually or hearing impaired consistent with Section 504 of the Rehabilitation Act of 1973. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the DOJ Website.

---

[2] Note that the decision to notify the media requires careful planning and execution so as not to unnecessarily alarm the public.

[3] As noted by OMB, e-mail notification is problematic, because individuals change their e-mail addresses and do not notify third parties of the change. If you do not have a mailing address and the affected person has provided you an e-mail address and consented to use of the e-mail address as a primary means of communication, notification by e-mail is appropriate.

3. Preparing for Follow-on Inquiries

GSA has a stand-by capability through its "USA Services" operation to quickly put in place a 1-800-FedInfo call center staffed by trained personnel and capable of handling individual inquiries for circumstances in which the number of inquiries is likely to exceed the agency's native capacity. (See Appendix B)

4. Preparing counterpart entities that may receive a surge in inquiries

Depending on the nature of the incident, certain entities, such as credit-reporting agencies or the FTC, may experience a surge in inquiries also. Thus, especially for large incidents, DOJ should inform the credit bureaus and the FTC of the timing and distribution of any notices, as well as the number of affected individuals, in order to prepare.

APPENDICIES

APPENDIX A

Sample Written Notification

DATA ACQUIRED: Social Security Number (SSN)

(Note: Do not insert actual SSN)

Dear :

We are writing to you because of a recent security incident at [DOJ or name of Component]. [Describe what happened in general terms, what kind of PII was involved, and what you are doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you complete a Federal Trade Commission ID Threat Affidavit at www.ftc.gov/idtheft. This will allow you to legally notify your creditors that your identity may have been compromised. Any debts incurred after that date will not be assigned to you.

We also recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personally identifiable information, such as home address or Social Security Number, that is not accurate.

If you see anything you do not understand, call the credit reporting agency at the telephone number on your report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identify theft. [Or, if appropriate, give contact number for law enforcement agency investigating the incident.] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you visit the Website of the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything [DOJ or name of Component] can do to assist you, please call [toll-free telephone number].

[Closing]

DATA ACQUIRED: Credit Card Number or Financial Account Number Only

(Note: Do not insert actual credit card or financial account numbers)

Dear :

We are writing to you because of a recent security incident at [DOJ or name of Component]. [Describe what happened in general terms, what type of PII was involved, and what DOJ is doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you immediately contact [credit card or financial account issuer] at [phone number] and close your account. Tell them that your account may have been compromised.

We also recommend that you complete a Federal Trade Commission ID Threat Affidavit at www.ftc.gov/idtheft. This will allow you to legally notify your creditors that your identity has been compromised. Any debts incurred after that date will not be assigned to you.

In addition, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personally identifiable information, such as home address or Social Security Number, that is not accurate.

If you see anything you do not understand, call the credit reporting agency at the telephone number on your report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identify theft. [Or, if appropriate, give contact number for law enforcement agency investigating the incident.] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you visit the Website of the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything [DOJ or name of Component] can do to assist you, please call [toll-free telephone number].

[Closing]

APPENDIX B

General Guidance for the Establishment of a Call Center in the Event of a Significant Data Breach

In the event of a significant data breach involving PII, the following guidance is provided to help with the determination of whether to establish a call center. The purpose of a call center is to provide individuals a number to call to obtain further information regarding the data loss and possible action they may want to take to lessen the incident's impact on their personal lives.

The decision to establish a call center should be based on several considerations:

- If a data breach does not extend outside of a Component (i.e., those affected by the breach are known and can be contacted), the establishment of a call center would not normally be necessary.
- If the breach affects a large number of individuals and those individuals are not easily identifiable or easily contacted, establishment of a call center should be considered to allow those potentially impacted to call and obtain additional information regarding the breach.
- Each situation will be unique and the decision to establish a call center must be based on individual circumstances. The main concern should be sharing of information with those affected and how they may obtain assistance.

Once a decision is made to establish a call center, there are several options:

- Contact the National Business Center to obtain a toll-free number. This option is likely the least expensive, since the DOJ will be providing its own personnel to support the call center.
- Contact the General Service Administration's (GSA) USA Services Group to establish a call center supported and staffed by GSA personnel. A statement of work (SOW) will be required and the call center can be up and running usually within 72 hours. SOW requirements can be found under "First Contact" at: http://www.usaservices.gov. A generic SOW is provided there. A thorough description of the incident and set of frequently asked questions (FAQs) will also be required for GSA personnel to refer to when fielding calls.

Suggested items to consider based on the nature of the breach would include, but are not limited to, the following:

- Using existing DOJ personnel to staff the call center and the number of individuals required
- Training of call center operators
- Pre-stage FAQs
- Ability to adjust staffing in response to call volume

- Daily hours of operations
- Cost of service
- Call logging
- DOJ reporting requirements
- Advertising call center numbers and making data breach information readily available to those affected
- Quality assurance checks of call center effectiveness

Sample call center FAQs are as follows:

1. How can I tell if my information was compromised?

   At this point, there is no evidence that any missing data has been used illegally. However, the DOJ/Component is asking each individual to be extra vigilant and to carefully monitor bank statements, credit card statements, and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved.

2. What is the earliest date at which suspicious activity might have occurred due to this data breach?

   The information was stolen from an employee of the DOJ/Component during the month of _____. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that individuals may notice suspicious activity during the month of _____.

3. I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself from being victimized by credit card fraud or identity theft?

   The DOJ/Component strongly recommends that individuals closely monitor their financial statements and visit the DOJ/Component special Website at www._____.gov.

4. Should I reach out to my financial institutions or will the DOJ/Component do this for me?

   The DOJ/Component does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts, unless you detect suspicious activity.

5. Where should I report suspicious or unusual activity?

   The Federal Trade Commission (FTC) recommends the following four steps if you detect suspicious activity:

   - Contact the fraud department of one of the three major credit bureaus:

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

- Close any accounts that have been tampered with or opened fraudulently.
- File a police report with your local police or the police in the community where the identity theft took place.
- File a complaint with the FTC by using the FTC's Identity Theft Hotline by telephone: 1-877-438-4338; online at www.consumer.gov/idtheft, or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

6. What is the DOJ/Component doing to ensure that this does not happen again?

The DOJ/Component is working with the President's Identity Theft Task Force and the FTC to investigate the data breach and to develop safeguard against similar incidents. The DOJ/Component has directed all employees to complete the DOJ "Computer Security Awareness and Training (CSAT)" course. In addition, the DOJ/Component will immediately be conducting an inventory and review of all current positions requiring access to PII and require all employees needing access to PII to undergo and updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI), depending on the level of access required by the responsibilities associated with their position. Appropriate law enforcement agencies, including the Federal Bureau of Investigation and the DOJ Office of the Inspector General have launched full-scale investigations into this matter.

7. Where can I get further, up-to-date information?

The DOJ/Component has set up a special Website which features up-to-date news and information. Please visit www._____.gov.

8. Does the data breach affect only certain individuals?

It potentially affects a large population of individuals. We urge everyone possibly affected to be extra vigilant and monitor their financial accounts.