NOTE WELL: THIS IS AN EXAMPLE OF OUR INTERNAL DOCUMENT USED FOR RESPONSE TO A COMPUTER COMPROMISE WITH POTENTIAL DATA LOSS WHEN THAT COMPUTER RESOURCE SCANNED RESULTS INCLUDED PERSONALLY IDENTIFIABLE INFORMATION (PII) RESIDENT SOMEWHERE ON THE DEVICE. YOU SHOULD CONSULT YOUR OWN INTERNAL POLICIES, PROCEDURES, PRACTICES, LEGAL COUNSEL, STATE AND FEDERAL REGULATIONS TO DEVELOP YOUR OWN TOOL-KIT OR BEFORE USING THIS AS A TEMPLATE.
I. OVERVIEW

A compromised computer found to have a positive Personally Identifiable Information (PII) scan on the machine at the time of a compromise may be subject to notifying individuals whose information was on the computer at the time of the compromise. Please read through the entire contents of this toolkit as it will describe what is considered to be notifiable PII and will outline the process to notify the affected parties involved. If there are additional questions, contact the Privacy Office, 814-863-7820 or privacy@psu.edu.

What is Considered Notifiable PII?
The Pennsylvania State Breach Notification Law applies to the data elements below when they are present in combination with the name of an individual (first and last or last and first initial):

- Social Security number;
- Driver's license number or a State identification card number issued in lieu of a driver's license;
- Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

1 Numbers that appear to be in the form of an SSN which start with an 8 or 9, such as Penn State ID Numbers, are not valid SSNs.
2 Please contact the Privacy Office with the other data elements which accompanied the bank account number to determine whether it is notifiable. Corporate bank account numbers are exempt and do not require notification.
3 Per Penn State practice, notification must be made regardless of whether there is a security code. If there is a name associated and a full card number, notification must be made. If the card numbers are in a merchant environment, please notify the Privacy Office (privacy@psu.edu) and Security Operations and Services (security@psu.edu) immediately. Corporate cards are exempt and do not require notification. Penn State P-cards involved should be reported to your local financial officer but are not considered to be notifiable PII.

Notification Timeline
It is important to understand the seriousness of these incidents and the need to immediately proceed with the steps outlined in this toolkit. This includes any collaborative effort with other offices. Penn State is obligated to comply with many federal and state regulations and business agreements. Failing to comply with such measures could result in fines, institutional reputation damage, loss of research grants, and other severe consequences.

Who is initially informed about a Compromise?
- Personnel listed as a network backbone contact for their respective department or area;
- Unit Director (Dean or Chancellor);
- Penn State Public Information Risk Management;
- Senior Management at the University Level.

What Costs May Be Involved?
- Forensic analysis (if applicable);
  - Forensic analysis may be required for any compromises which involve large files or more unique PII. Other circumstances may require a drive to undergo forensic analysis even if the total unique count is minimal, depending on the situation.
- Individual record searches for updated or unknown addresses (outside of Penn State Central Registry, if applicable);
- Third party notification services (if applicable);
- Individual credit monitoring (if applicable); and
- Other as applicable.
ROLE ASSIGNMENT

A. Unit Director (Dean or Chancellor)

The Unit Director is responsible for the following:

- Appointing a Project Manager
  - Reference the Toolkit to the designated individual(s).
  - Email the names and contact information of the designated individuals to the Privacy Office (privacy@psu.edu).

  The person chosen to handle the overall project (Project Manager) should be one who is:
  - Able to see the project through from start to finish;
  - Can serve as the liaison between the department and the Privacy Office, providing updates on status; and
  - Can identify immediate remediation efforts and appoint respective staff to handle notification.

  The point of contact chosen to handle the notification should be someone who is:
  - Understands and respects customer service;
  - Highly available the week notification is made and somewhat available for the week after, in order to respond to calls the same day they were received; and
  - Able to calm worried persons with accurate, consistent answers.

- Communicate with the Project Manager on progress.
- Sign notification letters.

B. Designated Project Manager (PM)

The Project Manager is responsible for the following:

- Ensure all responsibilities listed are assigned and completed.
- Oversee the project from start to finish.
- Make sure project takes priority and is completed in a timely manner.
- Remind all staff involved about confidentiality.
- Serve as the liaison between the department and the Privacy Office, providing updates on status.
- Identify immediate remediation efforts and appoint respective staff to handle notification.
- Work with the IT staff to obtain the offending PII and corresponding information.
- Obtain addresses of the SSN notification recipients (if applicable) as outlined in section III.2.
- Appoint or serve as the “point of contact”.
- Prepare and send the notification letters.
- Handle calls that result from the notification letters.
- Confirm the mail date with the Privacy Office.

C. Other Responsibilities [may fall under the Project Manager, computer user, information technology staff or another entity depending on the departmental appointment of such tasks]

- Confirm the detected Personally Identifiable Information (PII) has a name associated.
- Preserve and encrypt detected PII data files offline in a secure location in accordance with University Data Retention Policy AD 35.
- Rebuild the compromised computer (only after the detected PII files have been preserved and encrypted offline with prior approval/confirmation from the Privacy Office).
- Provide the PII data files to the Project Manager (PM).
- If PII is required to be stored, make sure it is done securely and that the proper authorizations are in place per University Policy AD-19 (http://guru.psu.edu/policies/AD19.html).
II. STEPS FOR NOTIFICATION

1. The Project Manager should work with the departmental-assigned delegate to extract the PII numbers and corresponding names of the individuals from the compromised computer. All PII numbers should be filtered for any duplicates before proceeding to step 2. Microsoft Excel offers a filter to sort through duplicates. Check with your local IT staff if you are not familiar with how this is done in Excel.

2. If SSNs are involved, the extracted SSNs only – not the names – should be sent to the Central Registry in an encrypted fashion. They will run a report against the registry and the returned results will either include a name and address or no values at all. If any values are returned as being “deceased”, notification is not required. The SSNs returned with no value must be matched with a name by looking in the original file. After a name is matched with the PII, encrypt the file and send it to the Privacy Office (privacy@psu.edu) to conduct an address search through another medium. Do NOT send all of the results from the registry report – only those which did not return a value. Make sure the name is included with the PII on the document you send to Privacy, if an address is needed. Depending on the amount of returned null values from the registry report, the department may incur a fee for the address search through the other medium which is utilized by the Privacy Office.

3. Prepare the notification letters by using the supplied letter template included in this toolkit. The Privacy Office will notify the user directly. The department; however, must send a formal letter to anyone other than the user, including any family members of the user.
   a. The department may utilize third party notification services; however, the associated costs will be borne by the department. For more information on the third party notification services, see Section IV.
   b. If the department desires to add or change any verbiage in the notification letter (other than those fields which can obviously be altered, as highlighted in yellow) – a copy must be sent to the Privacy Office (privacy@psu.edu) for approval prior to sending to the individual(s). Otherwise, the Privacy Office does not need to review the letter.
   c. The Penn State Public Information/ University Relations department is notified the same time as the Unit Director, Dean or Chancellor. Depending on the amount of PII involved or the sensitivity of the incident, Public Information may request a public announcement (example Penn State Live) be issued the day notification letters are sent. Each compromised computer case will be reviewed respectively and if determined a public announcement is in the best interest of the University, Public Information will work with the college on the verbiage prior to release. Calls from the media should not be handled by anyone other than University Relations, unless otherwise directed by the University Relations staff.

4. Mail the notification letters and confirm the date of the mailing by sending an email to the Privacy Office (privacy@psu.edu).
   a. Returned notification letters due to a bad or unknown address (or other reason) must follow these steps:
      i. Send the names and the corresponding PII of those which were returned to the Privacy Office (encrypt and send file to privacy@psu.edu) to see if there is another address available. If so, the letter must be resent. If not, preserve the returned letter with the other offending files. Do NOT send the returned envelop(s) to the Privacy Office.
      ii. If a third party handled the notification services for you, there is no need for a second notification attempt.
5. Confirm with the IT Staff that the files have been preserved properly – offline, encrypted, and secured in a locked cabinet and office, according to University Data Retention Policy AD 35, after notification has been made. Data files containing PII which did not require forensic analysis do not require full drive preservation; rather only the detected PII files, which can be placed on media that is moving forward with technology.

III. USING THIRD PARTY SERVICES FOR NOTIFICATION (mailing and call center services)

A. NOTIFICATION MAILING SERVICES

If the College is considering using the contracted third party notification services, please contact the Privacy Office to obtain a quote and overview of services. Such services include cross-checking addresses, preparing and sending notification letters and handling returned mail. Note the process of obtaining an address still needs to be done internally. However, any returned mail due to an unknown address can be handled by the third party.

Email or verbal approval to the Privacy Office (privacy@psu.edu) from the Unit Director, Dean or Chancellor is required to use the third party. Desired services must also be listed in the approval (mailing and/or returned mail management).

The following information will be required after approval is received from the Unit Director, Dean or Chancellor:

- **ENCRYPTED file with names and addresses (do NOT include Social Security Numbers)**
  - Confirm there are no blank address or name fields
- **ENCRYPTED digital signature of Dean or Chancellor**
  - Generally, methods for creating a digital signature include using a graphic tablet or signing a hard copy and scanning the signature. Clarity of the signature is important.
- **Copy of letter with all necessary sections completed** – make sure the name of the Unit Director, Dean or Chancellor is typed at the bottom of the letter the exact way it should appear on the letter (with title, Dr. or PhD if applicable)
  - Date incident occurred (to add to the letter)
  - Case number (to reference on letter)
- **Unit Director, Dean or Chancellor letterhead (electronic format)**

The information above should be sent to privacy@psu.edu. Do NOT send the decryption key in the same email; either call or create a new email. If there are any questions, please contact the Privacy Office at: 814-863-7820.

**NOTE:** The College is not permitted to outsource PII notification to any third party other than the company with which Penn State has a contract.

B. THE PENN STATE PRIVACY NOTIFICATION CALL CENTER

If wishing to use the Penn State Call Center Services, the FAQs in section VIII will need to be revised accordingly and provided to the Call Center Manager, along with a signed letter and a signed Consulting Service Requisition form at least one week prior to the mailing. The call center will be available to answer calls during the hours of 7:00am-10:00pm Monday-Friday and 8:30am-4:30pm Saturday and Sunday and most holidays.
IV. MALWARE NOTIFICATION LETTER TEMPLATE EXAMPLE

Note only minor modifications may be made to the letter; the final draft must be sent for approved through the Privacy Office, privacy@psu.edu.

[PLEASE NOTE: CHECK WITH YOUR LEGAL ADVISOR FOR YOUR SPECIFIC CONTENT REQUIREMENTS.]

ADD UNIT, DEPARTMENT OR COLLEGE LETTERHEAD

ADD DATE LETTERS ARE TO BE MAILED

Dear [NAME OF RECIPIENT]:

On [DATE OF INCIDENT] Penn State Security Operations and Services, a unit of Information Technology Services, alerted the [NAME OF DEPARTMENT] that a computer in the college had been infected with malicious software. A subsequent investigation on the computer involved revealed that your Social Security number [OR CREDIT CARD NUMBER, ENDING IN THE LAST FOUR DIGITS OF XXXX - IF APPLICABLE] was listed in a historical document on the computer. IF THIS LETTER IS FOR THE SPOUSE OR FAMILY MEMBER OF THE USER, INCLUDE THIS SENTENCE: It is likely your information became resident on the compromised computer because a family member of yours was the primary user. IF THE LETTER RECIPIENT IS A FORMER USER WHO PUT THEIR OWN INFORMATION ON THE MACHINE (no longer at Penn State), USE THIS SENTENCE: The compromised computer was one that you previously used while at Penn State.

The computer was taken offline as soon as the incident was discovered. We have no reason to believe that your information was accessed by unauthorized individuals. However, you should remain vigilant and promptly report incidents of identity theft to your local police department and to the Federal Trade Commission (FTC).

Enclosed is a brochure that details your rights and how to prevent identity theft. The enclosed information was compiled primarily from the FTC and the Pennsylvania Attorney General’s web sites. Please read this information carefully so that you can make an informed decision on measures you may want to take to help prevent identity theft. It is important to note that by placing a fraud alert through the credit reporting organizations, as described in the enclosed brochure (available at no cost), you will be alerted if someone attempts to use your identity to apply for credit. [IF CREDIT CARD WAS INVOLVED, ADD THIS STATEMENT: Additionally, we recommend you alert your credit card /bank card company. They will decide whether a replacement card should be issued.]

We are sorry for any inconvenience this may cause you. If you have any questions about this incident or any of the suggestions we have made, please contact [NAME OF PERSON HANDLING CALLS] at [PHONE NUMBER WITH AREA CODE] during the hours of [LIST DAYS AND TIMES]. IF YOU ARE USING THE PENN STATE CALL CENTER SERVICES, ADD THIS PART OF THE SENTENCE – …the Penn State Privacy Notification Call Center at 855-842-8351 during the hours of 7:00am-10:00pm Monday-Friday and 8:30am-4:30pm Saturday and Sunday.

Sincerely,

[Signature of Unit Director, Dean or Chancellor]

Enclosure: Privacy Notification

Add case number to bottom right corner – number only. This can be found on the email that was sent with the toolkit attachment.
V. PRIVACY NOTIFICATION BROCHURE

Information about Identity Theft Prevention

It is recommended that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and 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 the report.

Remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state’s attorney general and/or the Federal Trade Commission (“FTC”). You may contact the FTC or your state’s regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:
Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General’s Office:
North Carolina Attorney General’s Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies at the numbers above to find out more information.
I. FREQUENTLY ASKED QUESTIONS

GENERAL QUESTION TYPES RECEIVED

1. When did the breach occur?

2. Why did this take so long?

3. What does this letter mean? What really happened?

4. How did this happen? What is malware?

5. Am I the only one this happened to? I saw this on the local news - how bad is this, really?

6. What are you doing to make sure this won’t happen again?

7. What did I do wrong? What could happen to me, worst-case scenario?

8. Why was my SSN on the computer? I have no association with Penn State; I don’t understand why or how my PII was on a computer at Penn State.

9. Isn’t it illegal to have my SSN? What do I need to do?

10. Will you buy me “Free Credit Report.com” (or some other commercial service)? Do I need to cancel my credit cards?

11. Do I need to change my bank account passwords and debit card PIN? If I contact the credit reporting agencies mentioned in the letter, do I need to tell them my SSN?

12. If Penn State caused this, why should I have to take any action at all – why won’t Penn State take care of this for me? I have additional questions beyond the ones which were already addressed. Who can I talk to:

13. Will Penn State pay for my time in this? I’m going to sue Penn State/ I’m not happy with the resolution of this/ Who else can I speak with about this/ I have an unrelated question about Penn State. What type of information was in the file that is thought to be at risk?

14. I have no affiliation with the campus location who contacted me via a letter; I went to a different location at Penn State. Why was my information at this and how did it get there? What should I do after the 90 days from the original Fraud Alert?

15. What happens if we do notice suspicious activity? The privacy notification enclosure indicates a $10.00 fee is required to place a freeze on my credit. Do I have to do this?

16. Has my information been removed from the Penn State system? Yes, your information has been removed from the compromised computer.

The call should be ended with: Is there anything else I can help you with today? (assuming no) Thank you for calling [NAME OF DEPARTMENT OR PARTY HANDLING THE CALLS]