

Notification Letter Components (Section Two)



Other Toolkit Sections

[Toolkit Home](#) | [Section 1: Building a Press Release](#) | [Section 3: Incident-Specific Web Site Template](#) | [Section 4: Incident Response FAQ](#) | [Section 5: Generic Identity Theft Web Site](#)

Introduction

Edit the following components into a letter of notification or web site statement. Headings are boldface, several examples follow each heading. Delete the heading; edit the sample text into your letter.

Disclaimers: Don't disclose anything that hampers the investigation, gives additional information to those who would do harm, etc. Consult your university legal counsel. Release information only through university approved channels.



Hints

- 1) For printed notifications, ensure the letter appears genuine by printing it on colored letterhead paper, and mailing it in envelopes printed with your return address. If you have printed return address envelopes that are also security envelopes, that's even better.
- 2) If at all possible, individually address each notification. For printed notifications, format the letter so that the address of the recipient will appear in a window envelope. This will eliminate the additional step of printing the address on the envelopes and then matching the letters to the right envelopes. This will also allow you to use an electronic letter folder (borrow one from another unit if necessary) to fold the letters quickly for stuffing into the window envelopes.
- 3) As soon as you have a list of affected individuals, get someone to begin creating an address list in a standardized computer readable format (e.g. comma or tab separated CSV) that can be used to merge with letter text, print address labels and envelopes if necessary, and generate email notifications in an automated fashion. Gather all the necessary supplies for sending notification and arrange for postage while the letter is being finalized. Usually, the very last piece to be ready is the actual text of the letter.

i If you need help: There are a number of vendors who will handle all the aspects of notification for you, including identifying addresses for recipients, letter printing, envelope stuffing, and mailing. It is preferable to arrange for such services in advance of the need to notify, and this often can be done at no charge to you. But, vendors also will provide these services on demand at the time of the incident.

What happened?

(E.g., a server/laptop/desktop was breached/stolen/lost in <school or location>)

Example: In December 2004, campus officials were notified of the theft of an [department name] laptop computer

Example: . . . an on-campus server containing data on University international students was a target of computer hacking. As a result, these data were downloaded from the machine.

When did the breach occur and/or when was it detected?

Example: In December 2004, campus officials were notified . . .

Example: Late yesterday, the University discovered that on February 29, 2004 ...

How was it detected?

Example: "The university's routine, pro-active network scans detected an anomaly in . . ."

Example: "An employee in XYZ department reported unusual behavior in . . ."

Example: "A routine review of network activity logs revealed unexpected activity . . ."

What data was potentially compromised?

Example: This computer contained a list of [department] student employees. The list included the names and Social Security Numbers of the students.

Example: The data fields downloaded were: name, telephone number, University email address (if one was registered), social security number, date of birth, University identification number, passport number, city and country of birth, country of citizenship, school and department, degree sought, major field, University employee identification number (if employed at the University), non-immigration classification (e.g., F-1, J-1, etc.), and local and permanent address. Not all of these fields were filled for every student. It is also probable that a small number of students included in the database were domestic students who had been identified as international students prior to verification.

How much data was compromised?

Example: Although we have no evidence that an unauthorized individual has actually retrieved and is using your personal data . . .

Impacted Persons and the Information at Risk?

Why you are being notified.

Example: The file downloaded during this theft may have contained some information about you.

Example: We are notifying you of this security breach because you are one of the students whose personal information was present on the laptop. Although we have no evidence that an unauthorized individual has actually retrieved and is using your personal data, we are bringing this incident to your attention, in accordance with California law, so that you can be extra alert to signs of any possible misuse of your personal identity.

What steps are/were being taken?

(e.g. machine taken off the net, law enforcement (local/FBI), Credit card companies notified (for cases where contact information is needed about cardholders), etc)

Example: The server was originally secure but became vulnerable when a Microsoft security update to the operating system was installed. Security to the system has since been restored.

Several offices at the University, including Information Services and the Provost, are working hard to address problems caused by this incident and any further implications it might have for you. As the situation develops, we will send additional messages regarding further actions or precautions that you should take.

Is any data known to be fraudulently used or is notification precautionary?

What steps should individuals take?

(e.g., place a fraud alert with the credit bureaus, contact credit card companies, close accounts, etc.)

Example: Please monitor your email in the coming days for messages from The University.

Example: Although there is no evidence that an unauthorized person has obtained your personal information and is using it, there are some steps you can take, exercising abundant caution, to protect yourself. First, you may place a fraud alert with credit bureaus and/or periodically run a credit report to ensure accounts have not been activated without your knowledge. If you determine that an account has been fraudulently established using your identity, you should contact law enforcement and the financial agency. The following references provide additional information about identity theft:

- [Federal Trade Commission Identity Theft Web Site](#)
- Social Security Administration Fraud Line, 1-800-269-0271
- Major Credit Bureau Numbers
 - Equifax, 1-800-525-6285
 - Experian, 1-888-397-3742
 - Trans Union, 1-800-680-7289
- [Identity Theft Victim Checklist](#)

Example: Affected individuals are encouraged to:

- Obtain and carefully review credit reports. Order free credits reports from all three credit agencies by going to the website at <http://www.annualcreditreport.com/> or by calling 877-322-8228.
- Review bank and credit card statements regularly, and look for unusual or suspicious activities.
- Contact appropriate financial institutions immediately upon noticing any irregularity in a credit report or account.

Apology, expression of regret, or statement

NOTE: Apologizing for an incident could serve as an admission of guilt and create unnecessary risk to your institution, especially in situations where litigation might follow. Such a statement should be reviewed by General Counsel and Public Relations to ensure the institution is in agreement on whether or not an apology is appropriate. This is especially important if an incident is still under investigation.

Example: We deeply regret this situation and any inconvenience or alarm it may cause you.

Example: We regret that your information may have been subject to unauthorized access and have taken remedial measures to ensure that this situation is not repeated. The University is committed to maintaining the privacy of student information and takes many precautions for the security of personal information. In response to incidents of theft like this one and the increasing number of internet-enabled computer attacks, the University is continually modifying its systems and practices to enhance the security of sensitive information. We sincerely regret any inconvenience this incident presents to you.

Anticipated next steps, if any.

E.g., intention to notify if any additional information becomes available?

Example: The theft of this information raises a number of possible risks to you. One is theft of identity for financial gain. The University will be sending you a package of materials outlining steps you can take to protect yourself from this. Another risk is theft of identity for purposes of international travel or foreign entry. The University is currently working with several federal agencies, including the Immigration and Naturalization Service, and we have been informed that because of this theft, you may be asked further questions to verify your identity when leaving or entering the United States.


Who to contact for additional information

Contact/name, number, hours of availability, Web site, hotline, e-mail address, etc.

Example: Should you have further questions about this matter, please contact <name of contact>, <title of contact>, at <e-mail address of contact> or <phone number>.

Signature

Who makes most sense---president, dean, other contact familiar to the individual, consider multiple signatories for different constituent groups.

 Questions or comments?  [Contact us](#).

 *Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License* ([CC BY-NC-SA 4.0](#)).