

# Thresholds for notification

## Deciding Whether or Not to Notify

Campuses should consider the factors listed below in making a determination to notify for data breach incidents subject to state or federal notification requirements like the proposed "Identity Theft Protection Act" (S. 1408).

"The information" means data that would trigger the notification requirement like name in combination with SSN, driver's license number, and/or financial account numbers such as bank account or credit/debit card numbers i.e. information that could be used to commit identity theft.

1. Is the information is *in the physical possession and control* of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information?
2. Is there evidence that information has been *downloaded*, copied, or otherwise accessed, for example: an ftp log that contains the name of a file containing notice triggering information?
3. Was a privileged (e.g. root or administrator) or non privileged account, one with access to privileged information, compromised?
4. Was on system or multiple systems compromised?
5. Is the identity of the attacker known or unknown? If known was the attacker a disgruntled insider or an unaffiliated third party? Were multiple attackers involved?
6. Are there indications that the information was *used* by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported?
7. Did the unauthorized person have access to the information for an extended period of time?
8. What was the time between compromise start and compromise discovery?
9. Did the compromise indicate a directed attack, such as a pattern showing the machine itself was targeted versus an automated attack?
10. Did the attack appear to seek and collect the information?
11. Did the attack appear to include tampering with records (e.g., changing grades)
12. Did the attacker attempt to cover up their activity?
13. Did the attacker release information about the nature or scope of the attack?
14. Was the information encrypted and would the encryption method effectively prevent the information from being accessed.
15. What is the potential damage to individuals if notification is not given?
16. What is the potential damage to institutional credibility in the case of notification?
17. What is the potential damage to institutional credibility in the case of failure to notify?

## Acknowledgements

University of California Office of the President

[http://www.ucop.edu/irc/itsec/security\\_breach\\_notification.pdf](http://www.ucop.edu/irc/itsec/security_breach_notification.pdf)