EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 20, 2006

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Johnson
Deputy Director for Management

SUBJECT: Recommendations for Identity Theft Related Data Breach Notification

This memorandum provides recommendations for planning and responding to data breaches which could result in identify theft.

Over the past several months, the President's Identity Theft Task Force, established by Executive Order 13402 on May 10, 2006, has considered the steps agencies should take in responding to a data security breach which poses a risk of subsequent identity theft. The attachments to this memorandum reflect the work of the task force.

As you know, data breaches can implicate a broad range of harms to individuals, including the potential for identity theft. The crime of identity theft occurs when an individuals' identifying information is used by another without authorization in an attempt to commit fraud or other crimes. Identity theft undermines consumer confidence, harms our economy, and wastes consumer time, money, and effort to correct the damage caused by an identity thief.

To mitigate the risk of identity theft should a breach occur, I am recommending agencies establish a core management group responsible for responding to the loss of personal information as described in the attachment to this memorandum.

This memorandum does not address harms other than the potential for identity theft which could result from the breach of personally identifiable information. The Office of Management and Budget will develop additional guidance to address such issues and will incorporate as appropriate the recommendations in this memorandum.

Attachment

September 19, 2006

MEMORANDUM FROM THE IDENTITY THEFT TASK FORCE

Chair, Attorney General Alberto R. Gonzales ag
Co-Chair, Federal Trade Commission Chairman Deborah Platt Majoras DPM

SUBJECT: Identity Theft Related Data Security Breach Notification Guidance

The Identity Theft Task Force ("Task Force") has considered the steps that a Department or agency should take in responding to a theft, loss, or unauthorized acquisition of personal information that poses a risk of subsequent identity theft. This memorandum reports the Task Force's recommended approach to such situations, without addressing other notification issues that may arise under the Privacy Act or other federal statutes when the data loss involves sensitive information that does not pose an identity theft risk.

I. Background

Identity theft, a pernicious crime that harms consumers and our economy, occurs when individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes.[1] There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to commandeer an individual's existing accounts to make unauthorized charges or withdraw money. Second, thieves can use accepted identifiers like social security numbers ("SSNs") to open new financial accounts and incur charges and credit in an individual's name, but without that person's knowledge.

This memorandum describes three related recommendations: (1) Agencies should immediately identify a core response group that can be convened in the event of a breach; (2) If an incident occurs, the core response group should engage in a risk analysis to determine whether the incident poses problems related to identity theft; (3) If it is determined that an identity theft risk is present, the agency should tailor its response (which may include advice to those potentially affected, services the agency may provide to those affected, and public notice) to the nature and scope of the risk presented. The memorandum provides a menu of steps for an agency to consider, so that it may pursue such a risk-based, tailored response. Ultimately, the precise steps to take must be decided in light of the particular facts presented, as there is no single response for all breaches. This memorandum is intended simply to assist those confronting such issues in developing an appropriate response.

---

[1]Federal laws define "identifying information" broadly. *See, e.g.,* The 1998 Identity Theft Assumption and Deterrence Act (Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028)) and the Fair and Accurate Credit Transactions Act (15 U.S.C. §§ 1681-1681x, as amended). This memorandum focuses on the type of identifying information generally used to commit identity theft.

II. Data Breach Planning

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. Thus, an important first step in responding to a breach is for agencies to engage in advance planning for this contingency. We therefore recommend that each agency identify in advance a core management group that will be convened upon the identification of a potential loss of personal information. This core group would initially evaluate the situation to help guide any further response. Our experience suggests that such a core group should include, at minimum, an agency's chief information officer, chief legal officer, chief privacy officer (or their designees), a senior management official from the agency, and the agency's inspector general (or equivalent or designee). Such a group should ensure that the agency has brought together many of the basic competencies needed to respond, including expertise in information technology, legal authorities, the Privacy Act, and law enforcement. We recommend that this core group convene at least annually to review this memorandum and discuss likely actions should an incident occur.

III. Identifying an Incident That Presents Identity Theft Risk and the Level of Risk Involved

A loss of control over personal information, may, but need not necessarily, present a risk of identity theft. For example, a data report showing the name "John Smith," with little or no further identifying information related to John Smith, presents little or no risk of identity theft. Thus, the first steps in considering whether there is a risk of identity theft, and hence whether an "identity theft response" is necessary, are understanding the kind of information most typically used to commit identity theft and then determining whether that kind of information has been potentially compromised in the incident being examined. Because circumstances will differ from case to case, agencies should draw upon law enforcement expertise, including that of the agency Inspector General, in assessing the risk of identity theft from a data compromise and the likelihood that the incident is the result of or could lead to criminal activity.

An SSN standing alone can generate identity theft. Combinations of information can have the same effect. With a name, address, or telephone number, identity theft becomes possible, for instance, 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, if a PIN or security code is necessary to access the account; 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. For further purposes of this memorandum, information posing a risk of identity theft will be described as "covered information." If a particular data loss or breach does not involve this type of information, the identity theft risk is minimal, and it is unlikely that further steps

designed to address identity theft risks are necessary.[2]

Even where covered information has been compromised, various other factors should be considered in determining whether the information accessed could result in identity theft. Our experience suggests that in determining the level of risk of identity theft, the agency should consider not simply the data that was compromised, but all of the circumstances of the data loss, including

- how easy or difficult it would be for an unauthorized person to access the covered information in light of the manner in which the covered information was protected;[3]
- the means by which the loss occurred, including whether the incident might be the result of a criminal act or is likely to result in criminal activity;[4]
- the ability of the agency to mitigate the identity theft;[5] and
- evidence that the compromised information is actually being used to commit identity theft.

Considering these factors together should permit the agency to develop an overall sense of where

---

[2]OMB has promulgated guidance requiring certain notifications within the government, most notably to the United States Computer Emergency Readiness Team (US-CERT), whenever personal information is compromised, and which applies even where there is no identity theft risk. That reporting guidance remains in full effect.

[3]For example, information on a computer laptop that is adequately protected by encryption is less likely to be accessed, while "hard copies" of printed-out data are essentially unprotected.

[4]For example, as a general matter, the risk of identity theft is greater if the covered information was stolen by a thief who was targeting the data (such as a computer hacker) than if the information was inadvertently left unprotected in a public location, such as in a briefcase in a hotel lobby. Similarly, in some cases of theft, the circumstances might indicate that the data-storage device, such as a computer left in a car, rather than the information itself, was the target of the theft. An opportunistic criminal, of course, may exploit information once it comes into his possession, and this possibility must be considered when fashioning an agency response, along with the recognition that risks vary with the circumstances under which incidents occur. In making this assessment, it is crucial that federal law enforcement (which may include the agency's Inspector General) be consulted.

[5]The ability of an agency or other affected entities to monitor for and prevent attempts to misuse the covered information can be a factor in determining the risk of identity theft. For example, if the compromised information relates to disability beneficiaries, the agency can monitor its beneficiary database for requests for change of address, which may signal attempts to misuse the information, and take steps to prevent the fraud. Likewise, alerting financial institutions in cases of a data breach involving financial account information can allow them to monitor for fraud or close the compromised accounts.

along the continuum of identity-theft risk the risk created by the particular incident falls. That assessment, in turn, should guide the agency's further actions.

IV. Reducing Risk After Disclosure

While assessing the level of risk in a given situation, the agency should simultaneously consider options for attenuating that risk. It is important in this regard for the agency to understand certain standard options available to agencies and individuals to help protect potential victims:

A. Actions that Individuals Can Routinely Take

The steps that individuals can take to protect themselves will depend on the type of information that is compromised. In notifying the potentially affected individuals about steps they can take following a data breach, agencies should focus on the steps that are relevant to those individuals' particular circumstances, which may include the following:

- Contact their financial institution to determine whether their account(s) should be 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 might take a few months for most signs of fraudulent accounts to appear on the credit report, and this option is most useful when the data breach involves information that can be used to open new accounts. 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 free credit report can be used by individuals, along with the free report provided when placing a fraud alert (which is discussed below), to self-monitor for identity theft. The annual report also can be used as an alternative for those individuals who want to check their credit report, but do not want to place a fraud alert. Contact information for the credit bureaus should be provided, which can be found on the FTC's website.
- Place an initial fraud alert[6] on credit reports maintained by the three major credit bureaus noted above. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. After placing an initial fraud alert, individuals are entitled to a free credit report, which they should

---

[6]A fraud alert is a mechanism that signals to credit issuers who obtain credit reports on a consumer that they must take reasonable steps to verify the consumer's identity before issuing credit, making it harder for identity thieves to secure new credit lines. It should be noted that, although fraud alerts can help prevent fraudulent credit accounts from being opened in an individual's name, they also can delay that individual's own legitimate attempts to secure credit.

obtain beginning a few months after the breach and review for signs of suspicious activity.

- For residents of states in which state law authorizes a credit freeze, consider placing a credit freeze on their credit file.[7] This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. A credit freeze cuts off third party access to a consumer's credit report, thereby effectively preventing the issuance of new credit in the consumer's name.
- For deployed members of the military, consider placing an active duty alert on their credit file.[8] This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. Such active duty alerts serve a similar function as initial fraud alerts, causing creditors to be more cautious in extending new credit. However, unlike initial fraud alerts, they last for one year instead of 90 days. In addition, active duty alerts do not entitle the individual to a free credit report. Therefore, those placing an active duty alert should combine this option with a request for obtaining the annual free credit reports to which all individuals are entitled.
- Review resources provided on the FTC identity theft website, www.ftc.gov/idtheft. The FTC maintains a variety of consumer publications providing comprehensive information on breaches and identity theft.
- Be aware that the public announcement of the breach could itself cause criminals engaged in fraud, under the guise of providing legitimate assistance, to use various techniques, including email or the telephone, to deceive individuals affected by the breach into disclosing their credit card numbers, bank account information, SSNs, passwords, or other sensitive 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 him to a fake website whose only purpose is to trick the victim into divulging his personal information. Advice on avoiding such frauds is available on the FTC's web site http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt166.htm.

---

[7]State laws vary with respect to usability and cost issues, which individuals will need to consider before deciding to place a credit freeze.

[8]A variety of factors may influence a service member's decision to place an active duty alert–for example, if there are stateside family members who need easy credit access, the alert would likely be counterproductive.

B. Actions that Agencies Can Take

If the breach involves government-authorized credit cards, the agency 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, the agency should notify the bank or other entity that handles that particular transaction for the agency.

Agencies may take two other significant steps that can offer additional measures of protection – especially for incidents where the compromised information presents a risk of new accounts being opened – but which will involve additional agency expense. First, in recent years, some companies have developed technologies to analyze whether a particular data loss appears to be resulting in identity theft. This data breach analysis may be a useful intermediate protective action, especially where the agency is uncertain about whether the identity-theft risk warrants implementing more costly additional steps such as credit monitoring (see below) or where the risk is such that agencies wish to do more than rely on the individual action(s) identified above.

For two reasons, such technology may be useful for incidents involving data for large numbers of individuals. First, the cost of implementing credit monitoring (and the potential to have spent large sums unnecessarily if no identity theft materializes) can be substantial for large incidents because the cost of credit monitoring generally is a function of the number of individuals for whom credit monitoring is being provided. Second, subsequent to any large data breach that is reported publicly, it is likely that an agency will get reports of identity theft directly from individuals in the affected class. Yet, agencies should be aware that approximately 3.6% of the adult population reports itself annually as the victim of some form of identity theft. Thus, for any large breach, it is statistically predictable that a certain number of the potential victim class will be victims of identity theft through events *other than* the data security breach in question. Data-breach monitoring of the type described here can assist an agency in determining whether the particular incident it has suffered is truly a source of identity theft, or whether, instead, any such reports are the normal by-product of the routine incidence of identity theft.

Second, and typically at great expense, agencies may wish to provide credit-monitoring services. Credit monitoring is a commercial service that can assist individuals in early detection of instances of identity theft, thereby allowing them to take steps to minimize the harm (although credit monitoring cannot guarantee that identity theft will not occur). A credit-monitoring service typically notifies individuals of changes that appear in their credit report, such as creation of a new account or new inquiries to the file.[9]

---

[9]Various credit-monitoring services provide different features and their offerings are constantly evolving. Therefore, agencies may wish to consult with OMB or the FTC concerning the most current, available options.

In deciding whether to offer credit monitoring services and of what type and length, agencies should consider the seriousness of the risk of identity theft arising from the data breach. Particularly important are whether incidents have already been detected and the cost of providing the service. Such costs can be substantial, although rates are often subject to negotiation; bulk purchase discounts have been offered in many cases of large data breaches.[10] The length of time for which the service is provided may have an impact on cost as well. In addition, the agency should consider the characteristics of the affected individuals. Some affected populations may have more difficulty in taking the self-protective steps described earlier. For example, there may be groups who, because of their duties or their location, may warrant special protection from the distraction or effort of self-monitoring for identity theft.

Agencies should also be aware that, 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. Thus, an agency's contract officer, working with GSA, should be able promptly to secure such services and to develop cost estimates associated with such services.

Finally, it is important to note that notification to law enforcement is an important way for an agency to mitigate the risks faced by the potentially affected individuals. Because an agency data breach may be related to other breaches or other criminal activity, the agency's Inspector General should coordinate with appropriate federal law enforcement agencies to enable the government to look for potential links and to effectively investigate and punish criminal activity that may result from, or be connected to, the breach.

V. Implementing a Response Plan: Notice to Those Affected

Having identified the level of risk and bearing in mind the steps that can be taken by the agency or individual to limit that risk, the agency should then move to implement a response plan that incorporates elements of the above. Agencies 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 of identity theft 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. The private sector and other government agencies also incur costs in servicing these consumer actions. Moreover, frequent public notices of such incidents may be counterproductive, running the risk of injuring the public and, by making it more difficult to distinguish between serious and minor threats, causing citizens to ignore all notices, even of incidents that truly warrant heightened vigilance. Thus, weighing all the facts available, the risks to consumers caused by the data security breach warrant notice when notice would facilitate appropriate remedial action that is likely to be justified given the risk.

---

[10]In some instances, monitoring services may even be provided at no cost. Agencies should check the GSA contract schedule.

Assuming that an agency has made the decision to provide notice to those put at risk, agencies should incorporate the following elements into that notification process:

1. ***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. While it is important to notify promptly those who may be affected so that they can take protective steps quickly, false alarms or inaccurate alarms are counterproductive. In addition, sometimes an investigation of the incident (such as a theft) can be impeded if information is made public prematurely. For example, an individual who has stolen a password-protected laptop in order to resell it may be completely unaware of the nature and value of the information the laptop contains. In such a case, public announcement may actually alert the thief to what he possesses, increasing risk that the information will be misused. Thus, officials should consult with those law enforcement officials investigating the incident (which could include the agency's Inspector General) regarding the timing and content of any announcement, before making any public disclosures about the incident. Indeed, even when the decision has been made to notify affected individuals, under certain circumstances, law enforcement may need a temporary delay before such notice is given to ensure that a criminal investigation can be conducted effectively or for national security reasons. Similarly, if the data breach resulted from a failure in a security or information system, that system should be repaired and tested before disclosing details related to the incident.[11]

2. ***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 agency, or, in those instances in which the breach involves a publicly known component of an agency, a responsible official of the component.

There may be some instances in which notice of a breach may appropriately come from an entity other than the actual agency that suffered the loss. For example, when the data security breach involves a federal contractor operating a system of records on behalf of the agency or a public-private partnership (for example, a federal agency/private-sector agreement to operate a program that requires the collection of covered information on members of the public), the responsibility for complying with these notification procedures should be established with the contractor or partner prior to entering the business relationship. Additionally, a federal agency that suffers a breach involving personal information may wish to determine, in conjunction with the regulated entity from which it obtained the information, whether notice is more appropriately given by the agency or by the regulated entity. Whenever possible, to avoid creating confusion and anxiety, the actual notice

---

[11] There may be other reasons related to law enforcement or national security that dictate that notice not be given to those who are affected. For example, if an agency suffers a breach of a database containing law enforcement sensitive data, immediate notification to potentially affected individuals may be inappropriate – even if the risk of identity theft resulting from that breach is significant – as such notification may result in the disclosure of law enforcement-sensitive or counter-terrorism data.

should come from the entity which the affected individuals are reasonably likely to perceive as the entity with which they have a relationship. In all instances, the agency is responsible for ensuring that its contractor or partner promptly notifies the agency of any data loss it suffers.

3. ***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 agency's website and other information sites. 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 number, 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;
- steps individuals should take to protect themselves from the risk of identity theft (see above for the steps available), including steps to take advantage of any credit monitoring or other service the agency intends to offer and contact information for the FTC website, including specific publications.

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

4. ***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. First-class mail notification to the last known mailing address of the individual should be the primary means by which the agency provides notification. Even when an agency has reason to doubt the continued accuracy of such an address or lacks an address, mailed notice may still be effective. The United States Postal Service (USPS) will forward mail to a new address for up to one year, or will provide an updated address via established processes.[12] Moreover, certain agencies, such as the Social Security Administration and the Internal Revenue Service, may sometimes possess address information that can be used to facilitate effective mailing. The notice should be

---

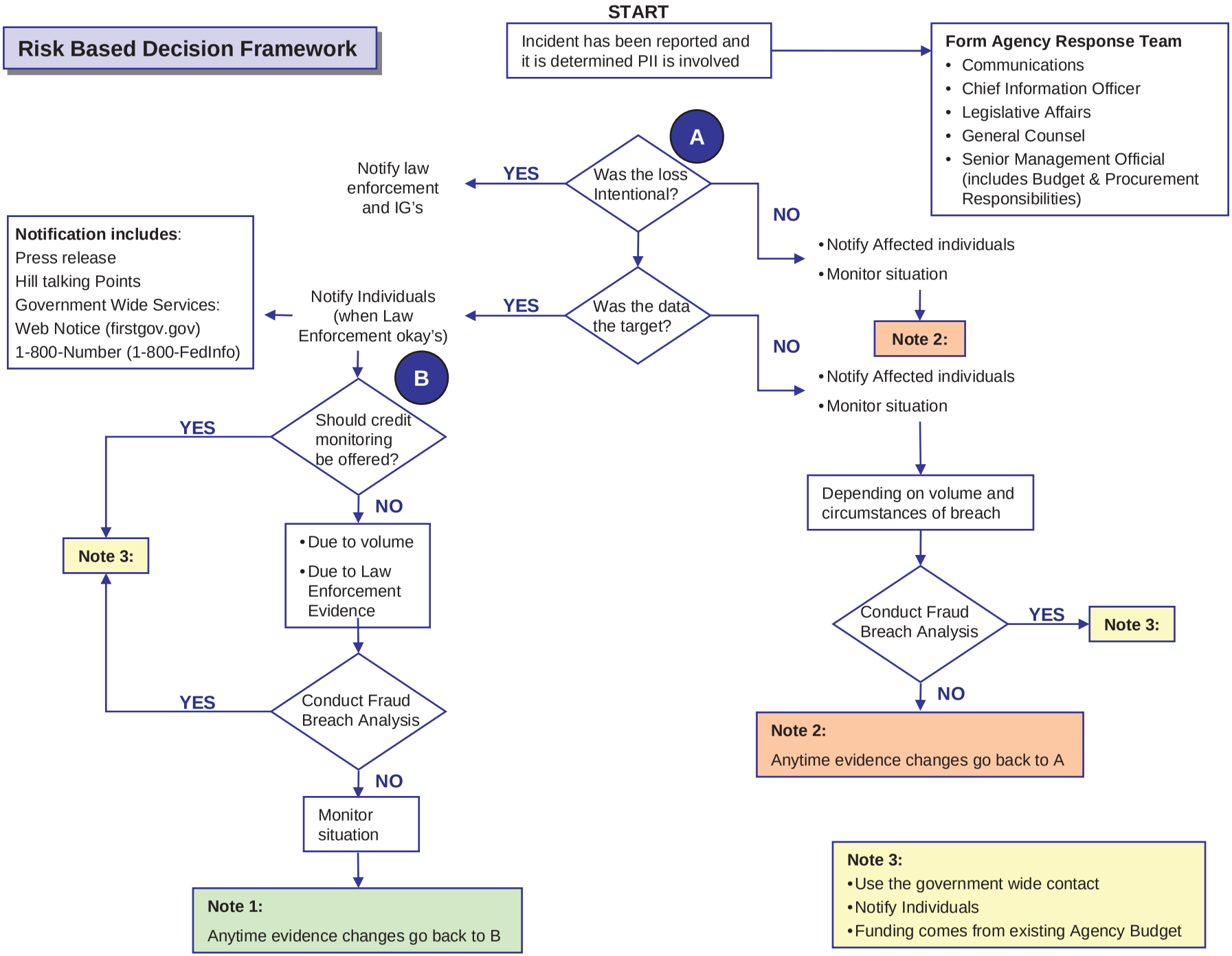
[12]Agencies may receive updated addresses as a mailer by becoming a direct licensee of the Postal Service or by using a USPS licensed NCOA Link service provider. A current list of service providers is available at http://ribbs.usps.gov/files/ncoalink/CERTIFIED%5FLICENSEES/. For information on address-update and delivery-validation services, contact the USPS at 1-800-589-5766.

sent separately from any other mailing so that it stands out to the recipient. If using another agency to facilitate mailing as referenced above, agencies should take care that the agency that suffered the loss is identified as the sender, not the facilitating agency.

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 individual class, should be employed to supplement direct mail notification or if the agency cannot obtain a valid mailing address. Email notification is discouraged, as the affected individuals could encounter difficulties in distinguishing the agency's email from a "phishing" email.

The agency also should 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 agency's web site.

5. ***Preparing for follow-on inquiries***: Those notified can experience considerable frustration if, in the wake of an initial public announcement, they are unable to find sources of additional accurate information. Agencies should be aware that the 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. Thus, agencies may wish to consider briefly delaying a public announcement to allow them to implement a consolidated announcement strategy, as opposed to a hasty public announcement without any detailed guidance on steps to take. Such a strategy will permit public statements, website postings, and a call center staffed with individuals prepared to answer the most frequently asked questions all to be made simultaneously available.

6. ***Prepare counterpart entities that may receive a surge in inquiries***: Depending on the nature of the incident, certain entities, such as the credit-reporting agencies or the FTC, may experience a surge in inquiries also. For example, in incidents involving a substantial number of SSNs (e.g., more than 10,000), notifying the three major credit bureaus allows them to prepare to respond to requests from the affected individuals for fraud alerts and/or their credit reports. Thus, especially for large incidents, an agency 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.

Risk Based Decision Framework