

The Deloitte logo is positioned in the top left corner of the page. It consists of the word "Deloitte" in a white, sans-serif font, followed by a small green dot. The background of the entire page is a photograph of a classical building facade with several large, white, fluted columns under a blue sky with scattered white clouds.

Deloitte.

Reducing Identity Theft.

*Make a Difference for Your Agency.
Make a Difference for America.*

Identity Theft and Your Agency – Why Should You Care?

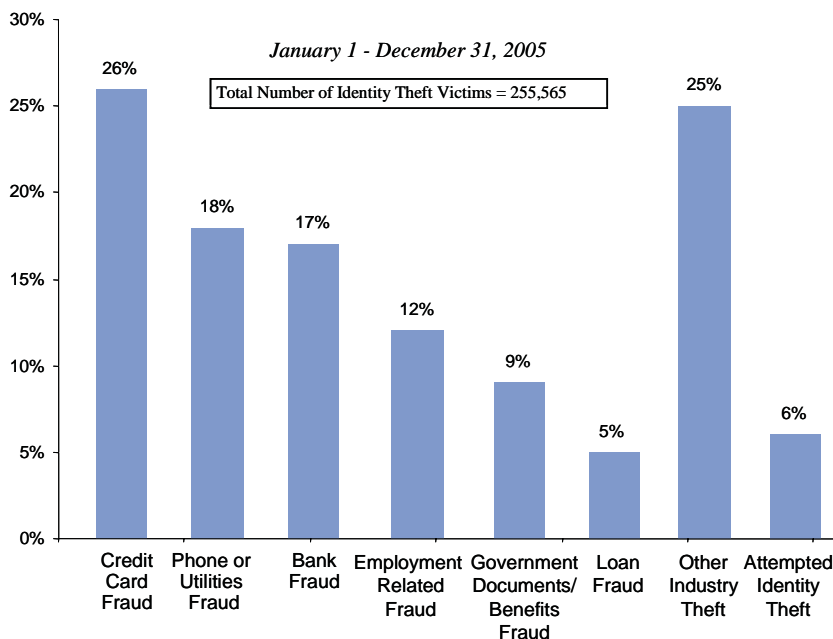
If you read the newspaper or watch television you already know the answer to this question. Whether an incident involves the loss of personal information about an individual whom your organization serves or the loss of your own employee data, identity theft significantly impacts the reputation of your agency and could put you in the position of having to defend yourself before the American public. In addition to suffering irreparable damage to your reputation, your agency could face budget cuts, incur the account management costs for theft victims or have to repay the losses themselves. How comfortable are you that your agency has done everything it can to reduce the threat of identity theft?

A Crime That Knows No Boundaries

Any organization that collects, stores, or has access to information about people is at risk of identity theft. A national crisis with global reach, identity theft is a facilitator of crimes that threaten international security, the economy, and personal privacy. It provides a way to remain anonymous, gain access, avoid detection, and transfer resources enabling organized criminal groups around the world to perpetrate heinous crimes such as terrorism, drug trafficking, and child pornography.¹ Identity theft has also been linked to methamphetamine addicts who have been especially adept at committing the crime to fund their drug habit.²

A multi-billion dollar national crisis, identity theft results in hardship for countless individuals and organizations on an annual basis. In April 2004, a survey by the U.S. Department of Justice estimated 3.6 million American households became victims of identity theft.³ Over the last decade the FTC named identity theft as one of the nation's fastest growing and most highly publicized crimes.⁴ How were stolen identities used? The FTC report, "Identity Theft Victim Complaint Data, Facts and Figures January 1 – December 31 2005", reflects that 9% of the data was used in Government Documents/Benefits fraud. The figure below illustrates other uses of identity theft victim data.

How Victims' Information is Misused



¹Percentages are based on the total number of identity theft complaints (255,565). Percentages add to more than 100 because approximately 20% of victims reported experiencing more than one type of Identity Theft. All victims reported experiencing at least one type of identity theft.

²Includes fraud involving checking and savings accounts and electronic fund transfers.

Federal Trade Commission
Released January 25, 2006

¹ Sullivan, Bob "Your Evil Twin – Behind the Identity Theft Epidemic" Pg. 77-82 & 200, John Wiley & Sons. Inc., c: 2004

² Sullivan, Bob "The Meth Connection to Identity Theft", MSNBC, March 10, 2004

³ U.S. Department of Justice, "Bureau of Justice Statistics Bulletin – Identity Theft, 2004," April 2006

⁴ Federal Trade Commission's, *Identity Theft Victim Complaint Data*, released January 25, 2006

Act Now...Or React Later

Whether an incident involves an involuntary breach of data or a thief who has already stolen an identity and comes to your agency for service, identity theft significantly impacts your agency's reputation and processes. It must be addressed proactively to minimize your risk.

Private sector organizations have responded in full force to the threat of identity theft. They have acknowledged that consumers have a choice among service providers—and that the mere perception of lax security or a potential risk is enough to influence consumers' decisions. The government has recently enacted legislation, presidential directives, identity theft incident reporting requirements, FY2006 FISMA agency privacy management requirements, and OMB initiatives (Memo 06-16, 06-19, and 06-20 addressing protection requirements for remotely stored sensitive data) as initial efforts to reduce and prevent future identity theft crimes at the federal level. These initiatives, as well as the introduction of the Identity Theft Task Force by the current administration, signals that the government realizes their responsibility to protect personal information entrusted to them by the public.

Given the evolving regulatory environment and the financial and reputation costs associated with identity theft, an increasing number of agencies are following the private sector's lead and adopting measures so as not to be taken by surprise should identity theft occur and they need to respond. These agencies understand the complexity and the far-reaching nature of this crime. They have learned that being proactive not only upholds their reputation in the eyes of the government and in the eyes of the American people, but also saves them time and money.

In the last 10 years significant efforts have been made toward streamlining many processes and moving to electronic services, with the goal of making the federal government more easily accessible to consumers. While this transformation from paper-based processes to "e-Government" is good from an efficiency perspective, it significantly increases agencies' exposure to the risk of identity theft. One example of a risk that agencies must deal with as a result of this transformation, is the unique authentication of users who attempt to log in to a website and access on-line services (e.g., request a refund, change address, etc.).

An organization's risk of identity theft can vary based on a criminal's ability to 1) exploit an existing vulnerability in a business process that can lead to the loss or exposure of personal information used by that process, or 2) use a stolen identity acquired from outside of an agency to successfully manipulate the normal function of your business process. Any sign that the public's data is less than secure may result in an increased demand for "face-to-face" interaction with the agency, thus returning to the previously used paper-based processes because of the perception that they are safer than online channels. This process reversal would significantly impact the efficiency of solutions already adopted by the agency, and increase the demand for resources to maintain the day-to-day operations further impacting cost.

The impact to an agency's employees should also be considered. While identity theft is more widely known as a crime that involves the theft of data of an organization's customers, the cost to adequately protect the data of an agency's employees is significant. Agencies are not only liable for any losses incurred to their employees as a result of a breach, but there may be an opportunity cost should employees fall victim to identity theft. The typical identity theft victim spends countless hours resolving personal problems due to identity theft—many of those hours expended during normal working hours. In fact, employers sometimes provide identity theft insurance to avoid being impacted should an employee become a victim.

In light of the evolving nature of identity theft crime, federal agencies will be required to quickly respond to a continuously changing regulatory environment. Responding to legislation and other government directives impacts an agency's resources available to conduct day-to-day business operations. This response is measured in a FISMA scorecard, and poor ratings indicate that an agency has failed to properly secure its information technology systems. This can adversely impact an agency in numerous ways from undermining public trust, to the delay or cancellation of OMB funding for agency programs.

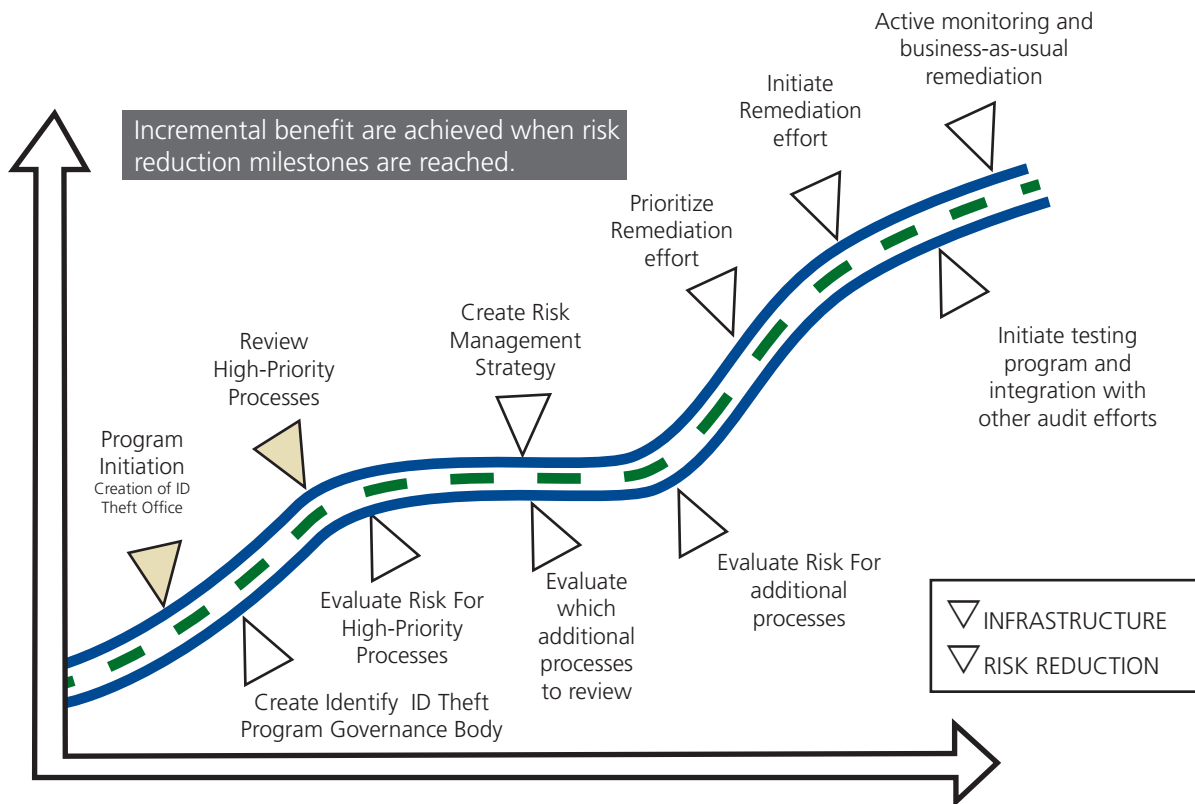
The proactive steps your agency takes against identity theft is as important in the public eye as how your agency responds in the event of a breach. Post-incident responses to identity theft incidents can be costly and time consuming. Responses have included credit checks on millions of individuals whose personal information was compromised, extensive investigations to determine culpability, and congressional or other oversight inquiries into an agency's safeguard activities. Taking preventative steps to address identity theft threat not only reduces the risk of incurring costs associated with activating an incident response plan and having to rebuild your reputation, but also builds public confidence by signaling that they can trust you with their personal information and you are committed to protecting them. Being prepared will lessen the overall cost to your agency, and help to prevent an identity theft incident before it occurs.

Know Thy Risk

Agencies must be vigilant in reducing their risk to identity theft. Although commonalities exist between a traditional security risk assessment and an identity theft risk assessment, security risk assessments focus on the risk associated with securing information technology systems while identity theft risk assessments focus on the entire business process with a specific focus on personally identifiable information. Assessing the identity theft risk to your agency requires more than a traditional systems oriented risk assessment; meeting security requirements and ensuring your organization is compliant with current regulation does not mean that you are safe against identity theft. Due to the multi-faceted nature of the crime, an identity theft risk assessment requires close examination of the business processes of your entire organization.

To provide value to agency decision makers, an identity theft risk assessment should be conducted by personnel experienced in utilizing a proven risk assessment methodology geared to understanding your agency's business processes and environment, information technology and manual systems, the regulatory environment, the governance model, and the unique nuances of identity theft as applied to your agency. Each organization, based on their business model, key stakeholder goals and risk tolerance level, has a unique set of vulnerabilities that must be prioritized by the level of risk they pose to the agency in order to build an effective identity theft program.

Road maps, such as the one below, are critical in building an effective identity theft program. Agencies should develop and tailor the road map based on the maturity of any existing identity theft program.



- ⇒ **Program Initiation.** The first step to building an identity theft program is to establish an identity theft office. The location of the office is entirely dependent on the focus of the agency. For example, if a particular business unit is the primary stakeholder, the office may be located in that unit; if the focus is on compliance, then the office could be located in the security, privacy, legal or risk management functions.
- ⇒ **Create Governance Body.** The governance body could either be a new body, or part of an existing agency governance body. In either instance, participants should include representation from all agency organizations that have a stake in the reduction of identity theft risk.
- ⇒ **Review High-Priority Processes.** Develop and use evaluation metrics that support the agency's business model in determining high-priority processes, initial identity theft risk assessment activities and the best use of assessment resources.
- ⇒ **Evaluate Risk for High-Priority Processes.** Conduct an identity theft risk assessment to determine initial risk levels and develop a risk mitigation strategy.
- ⇒ **Create Identity Theft Risk Management Strategy.** Create a risk management strategy that incorporates at a minimum, stakeholder, regulatory, and management goals and expectations.
- ⇒ **Review Additional Processes.** Review other business processes to determine candidates for additional risk assessment activities.
- ⇒ **Evaluate Risk for Additional Processes.** Conduct additional identity theft risk assessments to determine initial risk levels on the additional processes.
- ⇒ **Initiate Remediation Effort.** Based on the risk mitigation strategy, initiate remediation efforts that best meet agency risk reduction goals.
- ⇒ **Initiate Testing Program.** Develop and initiate a testing program to evaluate the effectiveness of selected identity theft mitigating or compensating controls.
- ⇒ **Active Monitoring/Business as Usual.** Incorporate identity theft activities and monitoring into existing processes including business, security, privacy, and system development life cycle processes.

Making a Difference

Identity theft is a crime against people—it impacts all of us. Because federal agencies maintain vast stores of personal information about people, they have a special duty to protect themselves from exposure. Think carefully about the impact of identity theft crime on your agency's reputation, your financial resources and staff, and on the people that your agency serves. Be confident that your agency's individual actions against this crime will make a difference for you, for your agency, and for the American people.

To speak to one of our identity theft specialists, obtain current and future research, or to receive information about public and private sector events around identity theft, please contact Lorna Joseph at ljoseph@deloitte.com.

Contacts

Joni Swedlund
Principal
Deloitte Consulting LLP
jswedlund@deloitte.com

Robert Jervay
Principal
Deloitte & Touche LLP
rjervay@deloitte.com

Hassan Afzal
Senior Manager
Deloitte Consulting LLP
hafzal@deloitte.com

Andrew Hartridge
Manager
Deloitte & Touche LLP
ahartridge@deloitte.com

Joe Brimacombe
Senior Manager
Deloitte Tax LLP
jbrimacombe@deloitte.com

Larry Chmiel
Manager
Deloitte & Touche LLP
lchmiel@deloitte.com

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas — audit, tax, consulting, and financial advisory services — and serves more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

In the U.S., Deloitte & Touche USA LLP is the member firm of Deloitte Touche Tohmatsu, and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Tax LLP, and their subsidiaries) and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting, and financial advisory services through nearly 30,000 people in more than 80 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's website at www.deloitte.com/us.