Opening Statement
Hearing: Fighting Fraud: Improving Information Security
Congressman John Shadegg

First, I would like to begin by thanking Chairman Bachus and Chairwoman Kelly for holding a hearing on improving information security. I also want to thank one of my own constituents, Mr. David McIntyre, President and CEO of TriWest Healthcare Alliance, for agreeing to testify.

My personal interest in identity theft began about five years ago when two of my constituents, Bob and JoAnn Hartle of Phoenix, Arizona, were victims of identity theft. My constituents were instrumental in getting the first state law in the nation to criminalize identity theft passed. Mr. and Mrs. Hartle suffered the devastation of identity theft when a convicted felon took Mr. Hartle's identity and made purchases totaling over $100,000. This individual also used Mr. Hartle's identity to obtain a security clearance to secure areas of Phoenix Sky Harbor International Airport and to obtain handguns using Mr. Hartle's clean record to go around the Brady gun law.

As a result of this victimization, Mr. and Mrs. Hartle were forced to spend more than four years of their lives and more than $15,000 of their own money to restore their credit because there were no federal penalties for identity theft. Their case led me to introduce a bill in the House that was eventually signed into law. The Identity Theft and Assumption Deterrence Act of 1998 gave law enforcement agencies the authority to investigate and prosecute identity theft crimes. Mr. and Mrs. Hartle also turned their unfortunate circumstance into something positive by establishing a non-profit organization to assist other victims of identity theft. Their website, www.idfraud.net is available to provide guidance to identity theft victims nationwide.

Identity theft ranges from individual instances like the Hartles' – involving small or large dollar amounts – to large organized professional crime rings. In fact, TriWest Healthcare Alliance, may well have been the victim of a professional operation. Like the Hartle's, Mr. McIntyre and his company took an unfortunate circumstance and turned it into a positive model for other companies to follow. Under Mr. McIntyre's leadership, on the morning of December 14, 2002, upon discovery of the break-in of their Phoenix office and the theft of computer hard drives containing their clients sensitive personally-identifiable information, TriWest Healthcare Alliance embarked on a journey to notify all 562,000 affected customers of the theft.

The stolen data included personally-identifiable information such as social security numbers, birth dates, and addresses from military personnel (one-quarter of whom are on active duty), retirees and family members who are served by TriWest under a contract with the Department of Defense. TriWest immediately reported the theft to the police, notified Department of Defense officials, and launched a 30-hour data run to determine what files were stolen. In addition, the company established a dedicated email address and set-up a toll-free telephone number with a three-tier response framework so customers would not experience wait times longer than one minute. TriWest mailed letters notifying victims of the theft and providing guidance on steps to take to protect their credit. TriWest also posted a $100,000 reward for information leading to the conviction of those responsible for the theft. In all, TriWest

undertook great efforts to notify the victims of the theft at a great financial expense to the company. Due to their extraordinary efforts, to date, no information from the purloined computer files have led to a single instance of identity theft.

The nature of identity theft has changed and the threat today is more likely than ever to come from breaches of data security. According to an identity-fraud manager at the Federal Trade Commission, there is a shift by identity thieves from going after single individuals to going after a mass amount of information. Law enforcement experts now estimate that half of all cases come from thefts of business databanks, as more and more information is stored in computer databases that are vulnerable to attack from hackers.

The identity theft legislation that I introduced and was signed into law in 1998 was an important first step in the road to crack-down on identity fraud crimes. However, more legislation is needed in this area to protect thieves from easily obtaining social security and credit card numbers from victims' mailboxes and waste containers left at the curb, to provide better coordination between victims and credit reporting bureaus, to establish procedures for businesses to follow in the event of a data security breach, and to provide stiffer penalties for criminals who steal and use another's identity. I look forward to hearing testimony from all of the witnesses to help identify areas in which a legislative response may be needed.

Chairman Bachus, Chairwoman Kelly, I thank you for holding a hearing on this important topic.