Testimony of

Mr. David McIntyre

November 4, 2003

Written Testimony of

David J. McIntyre, Jr.
President and CEO
TriWest Healthcare Alliance

Before the

U.S. Senate Judiciary Committee,
Subcommittee on Terrorism, Technology
and Homeland Security

November 4, 2003

Introduction

Chairman Kyl, Senator Feinstein and distinguished members of the Judiciary Committee, Subcommittee on Terrorism, Technology and Homeland Security. I would like to thank you for the invitation to appear before you today to discuss the important topic of identity theft. Unfortunately, this has become an increasingly prevalent issue and as consumers we are all concerned. I would like to thank you for the focus you are giving this critical issue and for your desire to enhance safeguards for consumers. In fact, a number of you have been involved in this issue for some time.

My name is David McIntyre. I am the president and CEO of TriWest Healthcare Alliance, a private corporation that administers the Department of Defense's (DoD's) TRICARE program in the 16-state Central Region and will soon do so across the expanded 21 state area known as the TRICARE West Region with the recent award of a 5 year - $10 billion contract that adds the states of California, Oregon, Washington, Alaska and Hawaii to those who already serve. We are the largest government contractor based in the state of Arizona, with soon to be substantial operations in California and these other states. The company I lead is privileged to serve the health care needs of those who have or currently defend our freedom and their families.

In mid-December, our company was the victim of a theft that placed at risk the personal

information of more than a half-million current and former TriWest customers (TRICARE beneficiaries), many of whom are also our employees.

As you know, identity theft is a serious federal crime that affects more and more Americans each year. This crime causes billions of dollars of harm to Americans each year. The thieves who commit these crimes against consumers don't just acquire merchandise illegally or use fake identification to obtain anything from a driver's license to a job; they wreak havoc on the lives of their victims. Repairing the damage done to a victim's credit record is costly and time-consuming. In fact, it often takes years for a victim of identity theft to clear up the mess created, and sometimes, their credit is permanently ruined.

In my opinion, there are few consumer issues more worthy of the attention of your Committee than this topic. And, on behalf of TriWest's employees and those we serve, I would like to commend you for your focus on this rapidly growing crime and the importance you are placing on the need for action. I am hopeful that your efforts will be successful and that they serve to enhance protection for America's consumers from this insidious crime. Accordingly, I am pleased to be here today to share the details of our story and to encourage you to take action to protect consumers.

I am particularly honored today to be in the presence of my home state Senator, Jon Kyl, and Senator Dianne Feinstein, both of whom have been important leaders in the effort to combat identity theft. I applaud your leadership on this critical consumer issue and thank you for the invitation to appear before you today.

TriWest Healthcare Alliance and the TRICARE Central Region Beneficiaries

TriWest is the Managed Care Support Contractor for the current 16-state TRICARE Central Region. We partner with the military to meet the health care needs of more than 1.1 million members of our nation's military family (active duty, their families, and retirees and their family members). And, as I stated, we are in the process of transition into five additional states - California, Oregon, Washington, Alaska and Hawaii. This territory includes 48% of the land mass of the United States, where we will provide services for some 2.6 million members of our nation's military family.

Based in Phoenix, Arizona, we have remote office locations across the 16-state Central Region. Most of our offices are on military installations.

TriWest has a strong history of collaboration and partnering with our military/ government

counterparts in the Central Region. In addition, we remain steadfastly amenable to providing information to the DoD, Congress, and Committees such as these, to the benefit of the TRICARE program overall, as well as the deserving population we serve.

As I have come to learn since December of last year, identity theft is the No. 1 consumer fraud in the nation. Nearly one million Americans were victimized last year alone. California ranks first in the country when it comes to the state with the greatest prevalence of identity theft; and Arizona ranks second. Given the impact on Americans who become the victims of these crimes, I believe this is an issue that demands action.

Due to the theft perpetrated against our corporation in mid-December, I have come to learn firsthand about identity theft. As a consumer, I now know the importance of keeping tabs on my credit files and billing statements in an effort to safeguard my personal information. As a business leader, I have learned that it is absolutely critical for companies to be more aggressive about security in all aspects of their operation.

Because TriWest is committed to providing exemplary service to those who sacrifice so much on our behalf, our Board of Directors, leadership team and staff at TriWest take a personal interest in matters that affect our customers. I am honored to be with you today to share what happened to us in mid-December, how we responded to the theft, and the invaluable lessons we have learned about identity theft. I hope that our sharing this information is helpful to you as you seek to determine what policy changes need to be made to provide optimal protection to America's consumers again this terrible crime.

Computer Theft at TriWest's Secondary Corporate Office

On Saturday morning, December 14, our secondary corporate office in Phoenix, AZ, was burglarized. Computer equipment and data files containing confidential and personal files of more than 500,000 members of America's military family were stolen from the premises. The information included on the stolen hard drives includes names, addresses and Social Security numbers, along with other personal information.

The burglary was discovered on December 16. Since that day, TriWest has coordinated closely with the authorities who are conducting the criminal investigation.

The identity of those who committed this crime and the motives behind the crime remain unknown. While information has been compromised, we do not have any verification that anyone's personal information has been misused or will be misused. The very possibility, however, that it could have been misused called for prompt action on our part to inform our customers about the compromising of their personal information and education about the steps they can take to protect themselves.

Health care professionals talk about the "Golden Hour" when they refer to the window in which it is critical that heart attack victims receive medical attention if they are to have high odds for survival and a reasonable quality of life. What I quickly discovered is that there is a "Golden Hour" when it comes to aiding consumers in protecting themselves against identity theft as well. The experts told me that if it we wanted the best chance of protecting our customers from

identity theft, we had no more than a couple of weeks to reach our customers and assist them in contacting the credit bureaus so they could act to place fraud flags on the credit files. In a case like this, a few weeks is the amount of time thieves would need to take the database and make credit instruments to perpetrate identity theft. Like the critical care needed for the heart attack victim, notifying our beneficiaries was the most effective course and it had to be done quickly.

It was this "golden hour" philosophy that guided our work and that of the Department of Defense in the days and weeks following the theft.

Coordinated DoD/TriWest Response to the Theft

From the day we discovered the theft, we began coordinating with our DoD partners. Once we had compiled the list of affected individuals from our backup tapes, we began working around the clock with the leadership of the DoD and the Military Health System to create and implement an integrated comprehensive communication plan.

The plan employed a three-prong approach that began with TriWest contacting the media to broadcast the theft and stress the need for individuals to protect themselves. Second, the DoD, working through the military commands, disseminated information to every installation, worldwide. The third component of the communication plan included a letter campaign that contacted every beneficiary affected by the theft, and which included information on steps they could take to protect themselves against misuse of their personal information.

Within weeks, the timeframe of the "golden hour" defined for us by the experts, the execution of this communication plan was complete.

I would like to share with you, in detail, the specifics of our efforts; however, I would like to first express my deep personal gratitude to the DoD for responding to this issue, and to Dr. Bill Winkenwerder, the Assistant Secretary of Defense for Health Affairs, for the immediate personal attention he gave the theft and the invaluable leadership he provided as we worked side-by-side with the other leaders throughout the Military Health System to deal with the situation. Without this coordinated response, our efforts to inform those impacted by the theft would not have been as successful.

This issue was a critical focus for our company. First and foremost, we believed it was necessary to alert the DoD, as well as the affected individuals, so that they could take action to protect themselves, should the thieves choose to misuse the personal information they illegally obtained. The following is a detailed account of the activities we were engaged in as a result of the theft. These include our ongoing efforts and reflect our continued commitment to respond quickly and aggressively to this issue:

? Authorities were contacted; federal investigators worked to find the individual(s) responsible for the crime.
? TMA and SAIC personnel analyzed what, if any, additional security measures should be taken to protect TriWest from another theft.
? The DoD began working with TriWest to ensure an uninterrupted delivery of medical benefits.
? I personally called the 23 beneficiaries whose credit card information was stolen. Information

regarding the theft was conveyed, and the beneficiaries were encouraged to take action to protect themselves from the misuse of their credit card. The beneficiaries were also provided contact information in the event they encounter any suspicious activity with their credit card.
? TriWest's proposed communication plan and messages were delivered to the Office of the Secretary of Defense (OSD) for review.
? All affected customers were contacted by mail to inform them of the theft and what the steps they needed to take to protect themselves from the possibility of "identity theft". Due to the fact that the credit bureaus are on different cycles for the update of fraud flags, with three months being the lowest common denominator, we have mailed our customers every quarter reminding them to update their fraud flag so that they will remain protected.
? A memo was distributed to all TriWest employees via email. Additional security policies were also distributed to all employees.
? The strategy for communicating the issue to beneficiaries was completed (with OSD approval).
? Ongoing communication updates were provided to TriWest's Board of Directors and subcontractors.
? Designated TriWest customer service personnel were trained to staff dedicated phone lines for incoming beneficiary calls.
? TriWest communicated with key Congressional leadership, Beneficiary Associations, and affected providers.
? Dr. Jerry Sanders, TriWest's Vice President of Medical Affairs and retired Deputy Surgeon General of the Air Force, personally contacted active and retired General Officers to inform them of the theft and our communication plan.

The communication strategy continued to be implemented throughout the holidays. By the end of December, TriWest had contacted each of the potentially affected individuals or families, and had also built a unique e-mail system, a web site and a call center to provide information and answer questions beneficiaries may have about the identity theft issue as well as the safeguards they can take to protect themselves. In addition, TriWest coordinated with the three credit bureaus to provide information on how to combat identity theft and place fraud alerts in their individual credit files.

Since the discovery of the theft, we at TriWest have taken measures to reconfigure our systems and enhance our security. In addition, we worked with federal personnel and a top private sector information security company to review all aspects of our physical and data security in an attempt to make sure that we understood all of the actions we should take to minimize the chance that such an event is repeated and we have taken those actions.

As a result of the break-in at our secondary corporate facility, we have learned a great deal about the issue of identity theft; it quickly became apparent to us how difficult it can be to catch those who commit such crimes. And, as it turned out, we were one of several health care and financial organizations in Arizona over a six month period that had been burglarized only to have the hard drives containing databases with personal consumer information stolen from their computers. In an effort to assist local and federal law enforcement in their pursuit of who was responsible for this crime, we posted the largest reward of its kind in the history of Arizona -- $100,000 for anyone who brought forward information leading to the arrest and successful prosecution of those responsible for this very serious federal crime -- a crime affecting more than 500,000 of

our nation's patriots. My Board and I had been hopeful that this $100,000 reward that we posted would encourage anyone that might know something to come forward and inform the authorities about the people responsible for this crime and the location of the stolen information. Unfortunately, that has not been the case.

The good news is that, to date, as far as we and the authorities are able to tell, no one's personal information has been misused as a result of the theft of our computer equipment and files.

Invaluable Lessons Learned

The theft of this computer equipment and the files contained within was and remains a matter of grave concern to everyone at TriWest as well as the DoD. As a result of the theft, and because it was the right thing to do, we became a more security-conscious organization.

We conducted a thorough security vulnerability assessment, took action to improve security across the enterprise, and, while I am not sure an organization can ever be fully immune to the risk of such thefts, we are confident we have contained further significant threats to our beneficiaries' personal information.

However, we will never become complacent with respect to maintaining the privacy of our beneficiaries.

The following are some of the steps we have taken to make sure nothing similar to this event ever happens within our organization again.

? TriWest has built an information technology infrastructure that includes enhanced security features.
? TriWest established a Security Steering Group with responsibilities to oversee data and physical security policies and practices throughout our corporation. The Security Steering Group reports directly to me as President and CEO. Specific duties of the Group include:
? Oversight of the IT security management program;
? Oversight of the execution of the company's Facility Security Plan; and
? Human Resources actions to include access privileges, background checks, and other classification actions including security awareness training for all personnel.
? TriWest has upgraded its incident reporting system.
? TriWest has received initial authority as part of the DoD's DITSCAP requirements (the DoD's security certification and accreditation process) and exceeded some implementation requirements by employing state-of-the-art security procedures.

Protecting Our Customers from Identity Theft

While we clearly suffered a burglary, and that was a significant concern, my greatest concern was what steps we could take to protect our customers from having the people who stole this equipment and the databases it contained from committing crimes against them by misusing the information to perpetrate identity theft.

In taking action, we researched information published by the Social Security and Federal Trade Commission (FTC) relating to information and identity theft. We developed a white paper, "Safeguard Yourself," as well as a telephone call center script that was based on the information we'd gathered. The paper included a description of the process our beneficiaries should employ to determine whether they are a victim of information or identity theft; how to initiate the placement of a fraud alert on their credit records; and how to contact each of the three credit bureaus in the United States. We submitted the paper to the attorneys in the FTC department that oversees identity theft and requested their review and suggested edits. They were extremely cooperative and helpful in reviewing the information we planned to provide our beneficiaries.

Following the review of our paper, one of the FTC attorneys, Naomi Lefkovitz, provided us with suggested contact points at each of the credit bureaus. We called each one to advise them of our situation and to seek their assistance and advice. They reported that the calls related to our theft caused a 300-400% increase in calls to their call centers.

A review of the calls received by our own Theft Hotline indicated that beneficiaries were asking whether TriWest could initiate the fraud alert with the credit bureaus on their behalf. This issue was a point of discussion between TriWest and the DoD; and a determination was made by the DoD Privacy Officer that, with permission of the person involved, we could initiate the fraud alert on their behalf.

Hence, discussions were held with each of the credit bureaus. TransUnion and Equifax agreed to accept requests, consistent with Privacy Act requirements, from us on behalf of beneficiaries. TriWest developed a plan that allowed beneficiaries to complete a request and authorization form on our web site, which was then transmitted to the credit bureau for their action. This process was implemented in an encrypted, secure manner. Experian determined that they would establish a web-based request for Fraud Alerts and an online viewing of the consumer's credit report. It was their preference for the consumer to enter their request directly into Experian's system via a hotlink from TriWest's web site.

Each of the credit bureau representatives noted that this was the first arrangement of this nature by their organizations on behalf of consumers.

This process is still in place. Upon receipt of the request and identifying information, the credit bureaus send a letter of notification regarding the fraud alert to the beneficiary, along with a copy of their credit report. (These arrangements were all made at no cost to the individual beneficiary.) The web request for fraud alerts was activated at the end of January 2003; since that time, over 63,000 beneficiaries have initiated fraud alerts.

Development of the web process for fraud alert requests made the process much more convenient for beneficiaries. By accepting batches of data files rather than thousands of calls to their call centers, it also served as a means of cost avoidance for the credit bureaus' call center operating costs. The credit bureaus were exceptionally helpful and responsive throughout this entire process, on both the technical and executive levels. Their advice, assistance, and cooperation have been noteworthy and extremely valuable.

And, as you may know, they have gone even further. They now share information on a regular basis... all to make processes easier for the consumer.

Needed Congressional Action

Without a doubt, we must rein in identity theft. Again that is why I am so appreciative of the focus that this Committee is giving to this critical consumer issue. Companies and consumers must take more aggressive steps to combat this crime and protect themselves. Based on all I have learned about this topic, I believe Congress needs to take action in three areas.

First, I very strongly believe that any organizational leader, be it public or private, whose organization suffers the theft of customers' personal information has an absolute obligation to inform those customers of such an event and help them understand what they can do to protect themselves against the misuse of that information. I understand personally the difficulty, cost and awkward nature of such disclosure, but to do anything less is wrong and indefensible.

After all, we are merely stewards of our customers' personal information as we seek to serve their needs. This is not our information; it belongs to our customers. And to not inform them of such an event for fear that we would lose their confidence or subject our company to negative publicity is unacceptable. It places our customers at even greater risk by preventing them from taking steps to protect themselves.

The safeguards that consumers can take to shield themselves from fraudulent uses of their personal information are uncomplicated and, if accomplished quickly enough after the theft, quite effective. Quick and decisive actions such as flagging your credit file, notifying your bank and other major creditors to watch for unusual activity and contacting the Federal Trade Commission to file a complaint can save years of expensive and time-consuming effort for consumers affected by such thefts.

It is for this reason that I appreciate Senator Feinstein's work in drawing attention to the issue and proposing constructive solutions with S. 1350, the Notification of Risk to Personal Data Act.

While some may suggest that we ought to simply leave it to organizations and the marketplace, to define the proper response to these incidents and the consequences for not taking appropriate action, I would suggest that this is neither fair nor appropriate for the consumer.

The "golden hour" in this area has been defined, and the consequence to the individual consumer of an organization not taking appropriate measures to inform them that their personal information has been compromised so that they can take measures to protect themselves places them at risk of individual financial ruin. We now know the effective ways to deal with this threat, and the credit bureaus have worked hard to put effective measures in place to support the consumer. Thus, I do not believe it unreasonable to say to those of us who have been entrusted with consumer information to meet the needs of our customers that the known theft or release of such information into the public domain triggers a requirement to arm the effected consumers with the necessary information so that they can take measures to protect themselves.

Second, as a consumer, I've observed the inconsistencies in how credit card numbers/accounts are handled among merchants. Specifically, I have noticed the variance in how credit card numbers are displayed on receipts. For instance, some receipts include the entire credit card number, expiration date and full name of the cardholder, which means the card number can now be used by anyone who happens to pick up the receipt. Other receipt slips contain only the last four digits of the credit card number, which offers more protection against misuse of the account. I believe that standardization of how credit card numbers are displayed on receipts, to block out most of the numbers, is one more way in which Americans could be better protected against identity theft, as it would help to minimize this type of criminal activity. I believe that the provisions contained in the legislation to reauthorize the Fair Credit Reporting Act, which I understand will be on the Senate floor for action soon, go a long way to address this issue and are worthy of your support.

And third, I believe the federal penalties for identity theft offer little deterrent to those bent on committing such a serious crime. For example, I was appalled to learn that the maximum federal penalty for such crimes is five years in prison and a $250,000 fine. These penalties must be significantly increased to serve both as an effective deterrent and a sufficient punishment. It is amazing to me that those who perpetrate such crimes often spend less time in jail than it takes the average consumer to clean up their credit. This has got to be fixed.

During the 107th Congress, lawmakers introduced more than two dozen bills to thwart identity theft and assist victims. Unfortunately, none of them made it into law.

I hope that the 108th Congress will be able to muster the support to move legislation in this area - strengthen the laws used to deal with those who perpetrate such crimes and enhance the protections for Americans.

Without question, the process of changing our laws is difficult. Our system of government requires careful deliberation, and that takes time. But thieves don't have to wait for public debate. They utilize new technologies as soon as they figure out how to profit from them. As a result, laws often play catch-up to technology. And, as our case and the others you will be hearing about today suggest, the criminals unfortunately have the upper hand.

Federal and state laws have yet to be tightened to provide law enforcement with effective enough tools to aggressively deal with the onslaught of identity theft. Unfortunately, in the breach lies the consumer. Identity thieves know that if they are caught, the current punishment is vastly inferior to, for example, robbing a bank. Yet, the impact of the crime is no less serious.

It is my hope that this Committee and Congress will be successful in championing the cause of strengthening the protections and penalties that predate the information age and take steps to modify the rules to add an effective layer of protection for all of us.

Conclusion

In an effort to protect our customers, we have dealt aggressively with this issue. We have communicated with all of the affected parties and the government. In addition, we have shared

this experience and the lessons learned with all of the Department of Defense Health System's contractors and the direct care system.

The criminal investigation remains active, led by the Defense Criminal Investigative Service and supported by the U.S. Attorney in Phoenix, the Federal Bureau of Investigation, and other law enforcement agencies.

We have been commended for our response to the theft and our honesty in communicating with those whose personal information was put at risk. In fact, we have received many words of praise from our beneficiaries. Of note, Chairman Myers of the Joint Chiefs of Staff, a former beneficiary of ours, whose name was included in the stolen data files, sent us a letter to applaud us for our immediate and responsive actions to the situation. While we appreciate the praise, all we did was respond by doing what we thought was the right thing by our customers who were infringed upon and whose financial integrity was placed at risk due to the burglary we suffered.

TriWest Healthcare Alliance takes great pride in the work that we perform. It is a privilege and a pleasure to support the Military Health System and the beneficiaries of the current TRICARE Central Region and the soon to be TRICARE West Region. These are the very individuals currently putting their lives on the line for freedom.

I am grateful that your Committee and its members are focused on this very important topic. The commitment you have made to learn about the threat of identity theft and take a proactive stance against its rampant spread is not only admirable but is also the bridge that is needed to make the public more aware of the potential every American is susceptible to, while sending a message to the criminals who perpetrate such insidious crimes. I would like to thank you for the opportunity to share this experience with you and provide information to you on this critically important topic.

Thank you for the invitation to participate in today's hearing. I would be glad to answer any questions that you might have of me.