
**Written Testimony of**

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

**Before the**

**U.S. House of Representatives Committee on Financial Services,**
**Subcommittee on Financial Institutions and Consumer Credit**
**and the**
**Subcommittee on Oversight and Investigation**

**April 3, 2003**

**David J. McIntyre, Jr.**
*President and Chief Executive Officer*

David J. McIntyre, Jr., president and CEO of TriWest Healthcare Alliance, is ultimately responsible for the successful operation of TriWest and the administration of the managed care support (MCS) contract in the TRICARE Central Region. Mr. McIntyre was the architect of the strategic vision on which the TriWest MCS proposal submission was based. He pulled together the shareholders and vendor subcontractors of TriWest, managed the development of the proposal, and oversaw the building of the company.

Mr. McIntyre has more than 18 years of experience, success and accomplishments in national health care policy development and business operations. He served for nearly nine years in the offices of the U.S. Senate, where he was responsible for health policy issues, most recently as a senior aide to Senator John McCain (R-AZ). As a vice president of Blue Cross and Blue Shield of Arizona, Arizona's largest health care organization, Mr. McIntyre managed numerous strategic projects including the development of TriWest and its MCS proposal, assisted with the management of the corporation's strategic planning process and had direct responsibility for legislative matters, media relations and several product development projects.

Mr. McIntyre has a master's degree in administrative sciences (with an emphasis in management and health policy/administration) from Johns Hopkins University and participated in the Executive Education Program for Senior Government Managers at Harvard University. He regularly addresses Arizona and national groups on health policy matters. He is past-president of the Arizona Association of Managed Care Plans (representing Arizona's managed care industry) and serves on the board of several Arizona health care entities. He was recently identified by Modern Healthcare magazine as one of 12 "Up and Comers" in health care for the Year 2000.

## Introduction

Chairwoman Kelly, Chairman Bachus and distinguished members of the Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit and the Subcommittee on Oversight and Investigations, I would like to thank you for the invitation to appear before you today to discuss the important topic of identity theft. Unfortunately, this is becoming 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, as I have come to learn, many of you have been focused for some time on enhancing consumer protection against identity theft.

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. We are the largest Department of Defense contractor based in the state of Arizona and are 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 has 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.

Identity theft is a serious federal crime that affects more and more Americans each year. In fact, this crime victimized nearly 1 million Americans last year alone. 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.

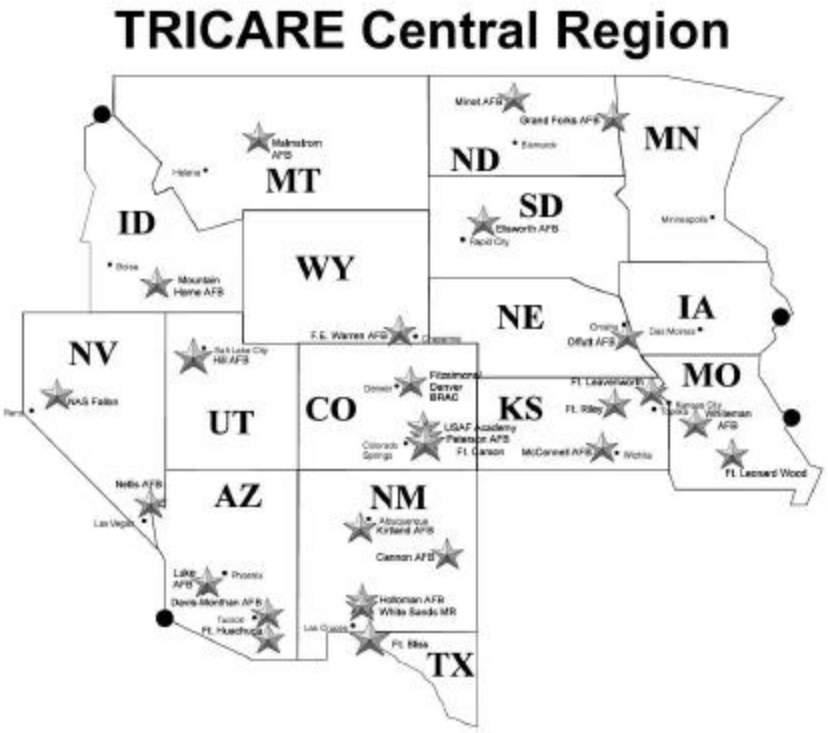
In my opinion, there are few consumer issues more worthy of the attention of your Committee than this topic. And, on behalf of TriWest's employees and those we serve, I would like to commend you for your focus on this rapidly growing crime and the importance you are placing on the need for action. I 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 some thoughts I have about action that could be taken to protect consumers.

I am particularly honored today to be in the presence of two of Arizona's Congressmen, John Shadegg from Arizona's 3rd District and Rick Renzi from Arizona's 1st District. I applaud their leadership on this critical consumer issue, particularly that of Congressman Shadegg who first started working on this issue 6 years ago, in response to the troubling experience of one of his constituents.

**TriWest Healthcare Alliance and the TRICARE Central Region Beneficiaries**

TriWest is the Managed Care Support Contractor for the 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).

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




● Areas not included in the TRICARE Central Region: Yuma, Ariz., contained in Region 10; six northern counties in Idaho contained in Region 11; certain ZIP codes in the St. Louis, Mo.area, and the Rock Island Arsenal area in Iowa, contained in Region 5.

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.

## 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.

Presently, the identity of those who committed this crime and the motives behind the crime are still 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 be 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.

## 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 a comprehensive communication plan to protect our beneficiaries.

The plan employed a three-prong approach that began with TriWest contacting the media to broadcast news of 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.

The execution of this communication plan is now 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 attention he gave the theft and the invaluable leadership he provided as we worked side-by-side with the other components of 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.

For the past three months, this issue has been 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.
- 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 have been working 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 understand all of the actions we should take to minimize the chance that such an event is repeated.

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. Therefore, TriWest posted a $100,000 reward in the hopes of assisting local and federal law enforcement to obtain 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. I remain hopeful that the $100,000 reward that TriWest posted will 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.

**Invaluable Lessons Learned**

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

We have conducted a thorough security vulnerability assessment, taken action to improve security across the enterprise, and, while there is more work still to be done, 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 happens within our organization again.

- TriWest has built an information technology infrastructure that includes enhanced security features. We have also hired an interim Chief Information Office, retired Navy Rear Admiral Todd Fisher.
- TriWest has 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.

**Challenges We Have Encountered and the Positive Results We Have Achieved**

TriWest 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; 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 have been 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.

Without a doubt, we must rein in identity theft. Again, that is why I am so appreciative of the focus that this Committee and its relevant Subcommittees are giving this issue. Companies and consumers must take more aggressive steps to combat this crime and protect themselves. Based on all I have learned these past weeks, I would suggest three additional measures.

First, any organizational leader, be they 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.

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.

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.

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.

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 punishment and penalties are a fraction of those for robbing a bank. Yet, the financial impact of the crime can be much greater.

It is my hope that Congress will champion the cause of strengthening penalties that predate the information age and take steps to modify the rules in the credit industry to add an effective layer of protection.

## 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 and openness 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, General Myers, Chairman 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 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. These are the very individuals who have or are currently putting their lives on the line for freedom.

I am grateful that your Committee and its Subcommittees are focused on this very important topic. The commitment you are making to learn more about 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.