In past articles, we've noted that SAIC has had a few compliance challenges. For example, in **this article** we wrote about allegations of bid rigging, and in **this article** we wrote about allegations of subcontractor kick-backs and timekeeping "irregularities" by an SAIC project manager. In the latter article, we wondered aloud whether SAIC's "notoriously decentralized and entrepreneurial" corporate culture may have contributed to the alleged issues caused by its rogue employees. Now comes another recent story involving yet another rogue SAIC employee. This time it may end up costing the company millions of dollars.

When this story first came to our attention, we frankly didn't think too much about it. Apparently, in September 2011, an SAIC employee had his car broken-into in San Antonio, Texas. His laptop was stolen. The laptop contained personal information (including healthcare information) of millions of military service members enrolled in the DOD's TRICARE program. TRICARE itself downplayed the risk, stating—

'The risk of harm to patients is judged to be low despite the data elements involved since retrieving the data on the tapes would require knowledge of and access to specific hardware and software and knowledge of the system and data structure.'

Ho hum. Just another data theft story. Or so we thought.But just a few weeks later, we ran across **this story** at NextGov.com. It reminded us that SAIC may be facing some rather large financial repercussions related to the data theft. The story reported—

Austin Camacho, a TRICARE Management Activity spokesman, said in a statement emailed to Nextgov that SAIC is 'contractually bound to mitigate the harmful effects of such disclosure. …'

Readers, reportedly *4.9 million people were affected by the data theft.* According to the TRICARE spokesperson, SAIC is contractually bound to mitigate the damages suffered by those 4.9 million people, including the generation of 4.9 million individual data breach notifications and the operation of call centers to address the questions and concerns of those affected. According to the NextGov article—

Larry Ponemon, chairman of Ponemon Institute, a research organization that specializes in privacy and data protection, estimated mail notification could run as high $7 per person, which means SAIC could face a bill of $34.7 million to notify all 4.9 million TRICARE beneficiaries.

But that's not all. In addition to the $34.7 million cost of notifying the affected people, SAIC may also be liable under statute for the data breach. The NextGov story reports—

The 2009 Health Information Technology for Economic and Clinical Health Act , enacted as part of the 2009 American Recovery and Reinvestment Act, specifies fines as high as $1.5

million for what it calls a breach of health care data.

Camacho said, 'The Department of Health and Human Services has the discretion to investigate the conduct of both the TRICARE Management Activity and SAIC and assuming it does so will ultimately make the determination as to whether and against whom it seeks to levy any penalties.'

So this rogue employee may end up costing SAIC at least $36 million. But that's not all.Just a few days later, the Department of Defense **was served** with a *$4.9 billion* class action lawsuit related to the data breach. According to NextGov (link in previous sentence)—

The suit … seeks $1,000 in damages for all 4.9 million TRICARE beneficiaries whose records were on the computer tape stolen Sept. 13 from the SAIC employee's car in San Antonio. TRICARE and Defense Secretary Leon Panetta are named as defendants. …

The suit …charges that TRICARE 'flagrantly disregarded' the privacy rights of TRICARE beneficiaries by failing to take the necessary precautions to protect their identity. The complaint said data on the stolen computer tape was 'unprotected, easily copied . . . [and TRICARE] inexplicably failed to encrypt the information.'

TRICARE 'compounded its dereliction of duty by authorizing an untrained or improperly trained individual to take the highly confidential information off of government premises and to leave unencrypted information in an unguarded car in a public location, from which it was stolen by an unknown party or parties,' the suit alleged.

The 'intentional, willful and reckless disregard of plaintiffs' privacy rights caused one of the largest unauthorized disclosures of Social Security numbers, medical records and other private information in recent history,' the complaint charged.

But that's not all. Just a few days later, SAIC was itself served with a similar lawsuit, also seeking $4.9 billion in damages plus free credit monitoring.

But that's not all. On November 7, 2011, NextGov **reported** that—

The TRICARE Management Activity on Friday directed Science Applications International Corp. to provide credit monitoring services for up to 4.9 million beneficiaries whose health information was stored on backup computer tapes stolen from an SAIC employee's car in San Antonio. … [TRICARE] directed SAIC provide one year of credit monitoring to patients who want it. SAIC will also analyze all available data to help TMA determine if identity theft occurs due to the data breach …

Providing credit monitoring services is not cheap. According to NextGov—

This could hit SAIC with a hefty bill if all 4.9 million beneficiaries whose data was on the stolen tapes ask for credit monitoring. When the Veterans Affairs Department experiences a loss, theft or exposure of this kind, it routinely offers credit monitoring services and up to $1 million annually in identity theft protection at a cost per veteran of $29.95 a year. If SAIC provided such monitoring and protection at the same rate, it would cost $146.8 million to cover 4.9 million people.

So, let's see now. We were at about $36 million or so. Plus $4.9 billion in potential legal damages. Plus $147 million in credit monitoring services. Hey SAIC, might want to rein in those rogue employees of yours. You know, the ones who can't be bothered to encrypt their laptop hard drives?