Data breach strikes fear into Utah victims

Data breach leaves Utah families scrambling to protect themselves.

By Kirsten Stewart | The Salt Lake Tribune
Published: April 24, 2012 07:26AM
Updated: April 24, 2012 08:24AM

As the mother of a 12-year-old girl with cerebral palsy, Christine Evans has learned to roll with the unexpected.

But everyone has their limits. And a week ago Evans reached hers after receiving notice that her daughter’s Social Security number had been compromised in a massive Medicaid data breach.

“It’s one more thing, as if I didn’t have enough to do,” said the working Tooele mother of three. “A lot of times we’re just keeping our head above water. To have this one more thing over our head, it’s drowning.”

Evans’ daughter, Camryn, is among 780,000 Utahns — many of them children on Medicaid — whose personal information was stolen by hackers on April 1 from a poorly protected Utah Department of Technology Services computer server.

State officials have taken steps to protect victims of the breach and guard against a problem like this happening again.

“We have worked around the clock to identify and notify people who had personal information compromised. Our top priority has been notifying individuals whose Social Security numbers were stolen,” said Utah Department of Health spokesman Tom Hudachko.

To date, letters have been mailed to 273,000 people.

But how many have taken advantage of the state’s offer of a year’s worth free credit monitoring isn’t
known. Without information from Experian, Hudachko could not immediately say on Monday.

Meanwhile, affected families are frightened, confused and far from certain that the state’s fixes will shield their credit and identities.

“I’m grateful for the credit monitoring,” said Evans, who out of precaution signed up all her children, even though Camryn is the only one on Medicaid. “But it’s just for a year. I don’t mean to be cynical, but what’s to prevent the hackers from waiting, holding onto Camryn’s information for a year and then using or selling it?”

Authorities, including the FBI, are still investigating, but traced the cyber crime to a computer in Eastern Europe.

The thieves probably weren’t interested in peoples’ health diagnoses, they say. It’s names, addresses, birth dates and Social Security numbers that have value to thieves, who can use the information to take out fraudulent loans.

Camryn has no need of bank accounts or loans, no cause to establish good credit.

Developmentally, the pre-teen is still a toddler. She can’t eat, bathe or get around on her own.

“But anybody could take her Social Security number and use it to gain employment and report that to the government, which might affect her eligibility for disabled services,” Evans said. “That’s vital stuff for us because that’s how she qualifies for Medicaid and gets respite care. And if something goes awry and it comes time to apply for Social Security disability when she turns 18, the feds can hold your application for up to five years. When you start thinking about it, it’s really overwhelming.”

As an added layer of security Evans looked into freezing her childrens’ credit.

“You can freeze the credit of a minor, but unless you have an open police report, you have to pay for it,” she said. “And if you go online you have a whole list of steps...I’ll have to carve out some time to do that, which hasn’t happened yet.”

Draper mother Heidi McKeever faced even more hurdles to helping her disabled daughter.

“I called to freeze Chloe’s credit, but because she’s 18 I had to explain to the guy [at Experian] why I was calling, I told him she is developmentally and intellectually challenged and that I’m her guardian. He said, ‘Oh, this is special circumstances,’ and put me on hold.”

McKeever was told she has to complete eight extra steps to get a power of attorney. To prove Chloe is who McKeever says she is, she has to find a piece of mail, preferably a utility bill, in her name. And, contrary to what state officials have said, the Experian representative said it’s not possible to permanently freeze Chloe’s credit.

“I understand things like this happen. But I’m frustrated that the process isn’t more streamlined, especially for people who are working on behalf of someone else,” McKeever said. “I hope the state uses this as a learning experience. You couldn’t find a more prime group of people to compromise, children and seniors and people with disabilities who don’t have the resources to rectify something if it happens. That part is sad.”

Low-income advocates agree and are pressing the Utah Department of Health to seek funding for an
awareness campaign to aid consumers and rebuild trust.

A state hot line offers little information other than what's contained in official notices to breach victims, said Judi Hilman, executive director at the Utah Health Policy Project. “And these notices are very long. I don’t know how many people are reading them.”

Consumers should have access to credit counselors with special care taken to reach out to those who are home bound, or don’t speak English, said Hilman. And state officials should consider re-branding Medicaid, which was stigmatized before the breach.

Tens-of-thousands of breach victims, however, have never been on Medicaid – people like Kimberly Wieling, who says St. Mark’s Hospital sent her personal information to the state without her permission.

The 53-year-old Holladay woman checked into the hospital’s emergency room last February with a lung infection. She was uninsured, due to her husband switching jobs, and planned on paying cash.

But after months of not seeing a bill, she called the hospital’s billing office, where staff said they were holding it pending approval of her Medicaid application.

“I said, 'I don’t have Medicaid. I’ve never had Medicaid,’” recalls Wieling. “She explained that anyone who comes to their hospital who does not have insurance, they automatically send it through the Medicaid system to see if they qualify.”

When Wieling complained she had never given the hospital permission to do that, she said, “The gal on the phone said, ‘Well, did you sign a letter to be treated?’

It just floors me. As far as I’m concerned, my Social Security number should never have been shared or exposed.”

HCA MountainStar, which owns St. Marks, issued a statement expressing sympathy for breach victims, but insisting that the hospital has no record of submitting a Medicaid eligibility query for Wieling.

“We understand why Ms. Wieling is concerned, and share her opinion that Social Security numbers should not be shared without permission. It is not our policy to do so, even while offering assistance to patients who are uninsured,” the statement reads. “Our records confirm that Ms. Wieling did not work with our representatives to apply for Medicaid, and we apologize for any misunderstanding that may have occurred when she contacted our billing office. Nevertheless, her information was compromised in the data breach, and we sincerely hope that actions taken by the state will protect her credit and identity, along with every other victim of this situation.”

kstewart@sltrib.com

Twitter: @kirstendstewart

Safeguard your credit

Will Vandertoolen, consumer services director at AAA Fair Credit, a federally certified, non-profit credit and housing counseling agency, says everyone – breach victim or not – should review their credit files at least once a year, at all three credit rating agencies.
“The worst time to find out you’ve been a victim of identity theft is when you’re applying for a much needed program or loan,” he said.

But no safeguard is foolproof.

Vandertoolen also recommends freezing your kids’ credit, which costs about $10 per agency. It costs about the same to unfreeze it.

Parents of children exposed in Utah’s Medicaid data breach may also consider petitioning the Social Security Administration for a replacement number. But this option is viewed as a last resort for people whose information has been abused.

“You have to prove you have taken other measures to remedy problems,” said Vandertoolen. “And some school and government records will need to be changed.”

For adults with extensive employment and credit histories, starting over is more complicated.

“You have to work with the credit agencies to update your files and make sure your employer and health providers know. If you’re in the military, it can throw up red flags and it complicates criminal background checks,” Vandertoolen said. “I didn’t know of anyone who has gone through with it.”

For more information, visit: Faircredit.org.

© 2012 The Salt Lake Tribune