Dr. Duane Thresher
250 4th Lane NE
Fairfield, MT 59436

February 19, 2015

To:

Montana Attorney General Tim Fox, 215 N Sanders Third Floor, PO Box 201401, Helena MT 59620-1401

US Attorney General, U.S. Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530-0001

FBI Director James B. Comey, FBI Headquarters, 935 Pennsylvania Avenue NW, Washington DC 20535-0001

US Senator for Montana Steve Daines, 1 Russell Senate Courtyard, Washington DC 20510

US Representative for Montana Ryan Zinke, 113 Cannon House Office Building, Washington DC 20515

Cc:

The Wall Street Journal Editor-In-Chief Gerard Baker, 1211 Avenue of the Americas, New York NY 10036

The Washington Times Editor John Solomon, 3600 New York Avenue NE, Washington DC 20002

Helena Independent Record Editor Greg Lemon, PO Box 4249, Helena MT 59604

Re:

Massive Healthcare.gov IT Security Breach, Criminal Negligence, Endangerment of Children, Montana Dept of Public Health and Human Services

To Whom It Should Concern:

We had to apply for health insurance through healthcare.gov Marketplace in December 2013 and using that information our child was, against our wishes, put on Montana's Department of Public Health and Human Services (DPHHS) health insurance in January 2014. We received the enclosed notification letter from MT DPHHS only on 10 July 2014; it was our and every parent's nightmare. Important excerpts are in quotes below.

"On May 22, 2014, an independent forensics investigation determined that an agency computer had been hacked. The forensic investigation was ordered on May 15, 2014 when suspicious activity was first detected by DPHHS officials."

"The information on the server may have included your child's demographic information, such as your child's name, address, date of birth, and Social Security number. The server may also

have included information regarding DPHHS services applied for and/or received in your child's name. Client information may include information related to health assessments, diagnoses, treatment, health condition, prescriptions, and insurance."

In clearer words, DPHHS let hackers access ALL our child's private information. This is exactly the nightmare worst-case scenario that everyone has been worried about with healthcare.gov Marketplace.

This not only happened to our child but thousands of other Montana children; those least able to protect themselves and least likely to complain, for fear of DPHHS reprisal.

As ludicrously-little mitigation (classic "bandaid on a bullet wound") DPHHS offered only the commercial services of the Experian credit reporting agency for a single year, as if identity theft were the only thing to worry about and only for a year (an identity thief will just wait the announced year and then will have probably years until the child turns 18 before anyone realizes the child has been harmed).

We, and other parents, are far more worried about the physical safety of our children since a child's stolen information would make abduction far easier. Lest you don't believe this is a real danger, in my IT work in Montana I discovered a registered sex offender, a pedophile, providing computers to libraries and possibly schools (library and school computer systems, which are usually insecure, have become prime targets for pedophiles). Further, over the years there have been numerous campaigns to teach children to be safe online to prevent just this danger from predators.

As an IT expert I have gone out of my way not to have information about my child online; for example, we have no Facebook page. Now all my caution about our child's safety has been thrown away by DPHHS's outrageous negligence. We will have to worry much more about our child's safety for many years now.

DPHHS claims its goal is to protect children and that all its clients have the right to have information they give to DPHHS kept private. Instead, on a massive scale, DPHHS has endangered children and violated their rights.

"at this time, we have no knowledge that any information on the server was used inappropriately, or was even accessed"

"we have no reason to believe that any information contained on the server has been used improperly or even accessed"

My wife and I used to be scientists and one of the first rules scientists learn is "absence of evidence is not evidence of absence", especially when one is motivated NOT to find evidence or is incompetent to do so, both as in this case.

Among other significant IT qualifications, I have a BS in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (MIT), a PhD in a supercomputing field from Columbia University and NASA, and I have worked at a Department of Defense supercomputing facility.

I came to Montana to start up a much-needed high-tech business, a secure data center, starting

with research for it (I was both encouraged and appalled when I first got here and found my local bank had a website on a Montana data center that was hacked). I have a small IT business on the side — computer networking, which is what IT is these days – but we have mostly lived off our savings (hence our low income).

What I have found in Montana is a severe lack of IT expertise but a huge resistance to letting any in. Employers either have no idea what it means to be qualified or give these good paying jobs to unqualified friends and relatives or won't hire people more qualified than they are.

According to just one of DPHHS's only two news releases (in May and June 2014) about being hacked, and not in the notification letter, "the server was likely first accessed in July 2013", 10 months before being discovered! Even that long period may be an underestimate since the competence of the suspiciously-unnamed people doing the "independent forensics investigation" is not known. If it took that long to discover, it was almost certainly just accidentally discovered and means DPHHS was not doing at-least daily computer security checks (e.g., checking logs), which is incredibly incompetent (if they did not know to do this or how to) or negligent (if they knew but didn't).

Then there is the issue of securing against vulnerabilities in the first place. Most people know little about computer network security and think these breaches are unavoidable. That is just wrong. Most hackers are not the computer geniuses portrayed in the media. They are amateurs just using widely-available easy-to-use tools to exploit well-known vulnerabilities that should have been closed when first made public. Not having closed these vulnerabilities, as is probably the case with DPHHS, is incredibly negligent and/or incompetent.

DPHHS's atrocious computer network security harms not only our child but me as well since much information given to DPHHS is about me and they have demanded a lot. For example, a Jennifer "L" out of the Choteau MT DPHHS office demanded my business records. That information would thus end up on DPHHS computers too so I had to refuse since I do computer network security and my clients' identities are confidential. Jennifer "L" won't give her last name and wants to do things by phone not in writing, which is absurd since this is exactly what a child abductor would try. (Security starts with being sure who you are dealing with.) Moreover, Jennifer "L" is probably the person who has started numerous different healthcare.gov Marketplace applications in our child's name without our permission or advance knowledge, which is identity theft and should be investigated.

(DPHHS's physical information security is also lax — often sensitive information mailed from DPHHS comes in envelopes that are open, having never been sealed.)

The first signer of the DPHHS-hacked/child-endangered notification letter is Richard H. Opper, Director of DPHHS, appointed by MT Governor Steve Bullock in December 2012. He has no real IT qualifications, just old degrees in soil and agriculture. Maybe one could weakly argue he doesn't need any – although these days it's obvious it should be a requirement – but as director he certainly bears major responsibility for this disaster since he at least negligently hired (without due diligence) the negligent or incompetent IT workers. Moreover, he is clearly not interested in being director of the state's largest agency, tasked with protecting children. His public LinkedIn page is mostly about his unsuccessful writing career. During the time he should have been protecting Montana's children he was apparently busy writing a book with

the storyline "Will a chance encounter with a homeless man leave Kelvin with true love and success or destroy his whole life?"

The other signer of the letter is Ron Baldwin, MT State Chief Information Officer (CIO), appointed by MT Governor Steve Bullock in January 2013 but previously CIO for DPHHS. Given the uncertainty it is quite possible he was DPHHS CIO when it was hacked; he may have at least set the stage for it before he left. There is no question he should have significant IT qualifications. Baldwin's only IT qualification is an associate's degree in computer science from a community college in 1982, more than 10 years before the "Internet" and around the time of the first PCs. Moreover, community colleges, as well as for-profit educational institutions, are the leading culprits in producing unqualified IT workers since they have to employ as teachers IT workers just like everyone else and so have the same mentioned problems hiring qualified ones.

After Ron Baldwin, and currently, Stuart Fuller is CIO of DPHHS, probably hired by Richard Opper. He was there when the breach supposedly first occurred. Again, there is no question he should have significant IT qualifications. Nothing can be found about his IT qualifications, which probably indicates he has little or none worth mentioning publically.

Although these men can't shirk their responsibility for this disaster since they are legally required to do due diligence, they may try to blame, probably namelessly, the negligent or incompetent IT workers they hired, perhaps a contracted company. If so, the names and qualifications of the individual IT workers hired should be made public and they should ALSO be individually held responsible and punished for their negligence.

There has been some brief talk in Congress of the security of healthcare.gov Marketplace, with ignorant assurances that it is perfectly safe. What was not considered was that when healthcare.gov Marketplace included state health insurance systems in their system they accepted responsibility for the security of those state systems as well. This makes the MT DPHHS hacking a federal matter too.

"As soon as the suspicious activity was discovered, agency officials immediately shut down the server and contacted law enforcement."

It suspiciously does not specify what law enforcement was contacted but it was probably local. Since it is now also a federal matter the FBI and US Attorney General should also be involved, along with the MT Attorney General.

Obviously the hacker was never found and he was probably not even looked for — and no, it's not impossible to find them. But if he had been found, criminal charges, with significant prison time as punishment, as well as large monetary penalties, would have been brought against him.

Letting him hack DPHHS is criminal negligence, endangerment of children, by at least all those discussed above. Considering that there were thousands of victims and these victims were children, state and federal criminal charges should be brought against them, with significant prison time as punishment, as well as large monetary penalties (consider that Ron Baldwin's salary is $111,000; Richard Opper's and Stuart Fuller's are about this). We demand this.

Failure to do so clearly demonstrates a lack of concern for the safety of children. Besides also

just being the right thing to do, doing so has some positive benefits as well. First, it will prevent some of the many lawsuits, with awards totalling many millions of dollars, against the state and federal government that are sure to come and be readily won by the victims. It will also lessen the scourge of IT security breaches from negligently hiring incompetent IT workers since finally there will be some individual responsibility and real consequences for them. Finally, Montana's reputation will be redeemed and it will attract the IT expertise and investment in IT infrastructure it so badly needs.

Those in the FBI who are IT-qualified should investigate. I also demand to be allowed to see the evidence myself since I am at least as IT-qualified and so that I can best protect our child.

It's obvious Richard Opper, Ron Baldwin, Stuart Fuller and the others should also be immediately fired, lose all pensions and benefits, and be barred from further government jobs. Montana's CIO is the head of the Montana State Information Technology Services Department (SITSD), which is responsible for other important state computer systems. Having Ron Baldwin being MT CIO is foolishly dangerous and negligent.

I can provide more documentation of all of the above and more. Obviously I can't trust doing this over the phone now but if mail is too slow I can be reached at @threshernetworks.com. If you know how I would prefer to receive and send signed and encrypted email. I would use my personal email address from my local ISP, 3 Rivers Communications, but I have discovered that email from government and conservative organizations is often filtered without notification by 3 Rivers. 3 Rivers is another example of the many serious problems caused by negligently hiring incompetent IT workers.

Sincerely,

Dr. Duane Thresher
PhD, Columbia University and NASA
BS, Massachusetts Institute of Technology (MIT)

encl.: DPHHS-hacked/child-endangered notification letter of 10 July 2014