

June 13, 2005

## **U.S. Offshoring of Personal Data Grows**

*Diane M. Grassi*

According to the Identity Theft Resource Center in San Diego, CA there have been close to 60 reported security breaches of customer financial information from United States corporations thus far in 2005, involving 13.5 million customers' identities. The companies include Choicepoint, Inc., Bank of America Corp., Wachovia Corp., Ameritrade Holding Corp., DSW Shoe Warehouse, Time Warner Inc., LexisNexis and most recently Citbank Financial Group. While most lost data has involved data storage tapes lost in transit by courier services or UPS, others involved computer security breaches. And as corporate America looks for ways to shore up its security problems rather than face the wrath of Congress, an even more unwieldy problem is brewing abroad.

As holes still exist in protecting the personal information of both customers and employees of corporations in the United States, many of these same corporations, which include the largest financial institutions and two of the three credit reporting agencies, have offshored information technology units which include-back office functions from customer service to software development and engineering.

Yet American customers or consumers are never informed whether or not their personal information and credit history is being offshored, as it is not required by U.S. corporations to do so. Coming to light is that various U.S. government programs and states are utilizing more and more offshore subcontractors in addition to those corporate entities which indirectly do business with the U.S. government. But unknown to the American consumer or taxpayer is the threat of theft of an individual's identity and financial resources which remain largely unprotected without the ability to enforce U.S. law on foreign land.

Accounting firms are offshoring IRS tax preparation. The U.S Department of Agriculture defers to the states to run food stamp programs, with as many as 43 states offshoring call-centers to India even though federal law dictates that only U.S. government workers should handle the job. The Health Insurance Portability & Accountability Act (HIPAA) which protects the health information of a patient and prevents healthcare companies from selling such information to third parties such as telemarketing firms, does not limit nor prohibit the transfer of information to overseas locations for third party subcontracted services. And many public and private hospitals are sending diagnostic radiology work to India with no law requiring notification to patients that a radiologist in India, unlicensed in the U.S., is reading x-rays and diagnosing illnesses and injuries. Known as "ghosting," U.S. certified radiologists oversee radiologists in India while x-rays are electronically transmitted. Initiation of regulatory controls is only now in the beginning stages to ensure doctors performing such work are properly trained.

As overseas contractors and subcontractors are outside the jurisdiction of U.S. consumer privacy laws that protect medical and financial information in the U.S., corporations have little recourse in the outsourced host country if a violation of security or theft occurs. India's IT Act of 2000 does not address the issue of privacy protection and regulation of the use of data. It only covers unauthorized access and data theft directly from computers and networks. Indian law does not cover data interception and computer forgery or fraud at all and no legal remedies in India yet exist for such enforcement.

In the U.S., the Gramm-Leach-Bliley Act of 1999 which applies to financial institutions as well as accounting firms engaged in the practice of tax preparation requires that firms design, implement and put safeguards in place in order to maintain protection of customer information. In addition, such companies must provide their customers with a privacy notice that details the company's information-collection and information-sharing practices giving the customer the right to "opt-out" and limiting the sharing of such information. Yet to date the Federal Trade Commission has not levied any punishment or fine on any U.S. accounting firm with regard to overseas outsourcing practices and the lack of notification of such to customers.

A growing trend in the legal profession is the overseas outsourcing of paralegal services including legal research. Some of the country's largest law firms are utilizing such services. According to John Halvey of New York-based Milbank, Tweed, Hadley & McCoy, "I can't think of a recent deal we did that didn't have an offshore component." But issues of attorney-client privilege create limitations on what may or may not be outsourced by a law firm, especially without the consent of law firm clients.

While the U.S. federal government invests more resources into tightening security in a post-9/11 world, multi-national corporations put the U.S. infrastructure at greater risk through offshoring maintenance and development. There are very few areas of information technology which do not impact the operation of infrastructure in the U.S., which in some ways have direct implications on homeland security. Financial and accounting institutions have now been joined by software programmers maintaining operations for U.S. based health care providers, airlines, railroads, power companies and defense contractors, all of which subcontract offshore.

Outsourcing computer networks offshore creates an immediate liability as there no longer is direct company control of data due to dependency on service providers abroad with neither the outsourcing vendor nor the outsourcing client knowing the exact path the data takes. **For example, AT&T's switched network carries economic, financial and military communications, which accounts for a great deal of the foundation of U.S. infrastructure, and relies on programming and maintenance from engineers offshore.** Pacific Gas & Electric of California, one of the U.S. companies responsible for maintaining and upgrading the U.S. electrical grid, outsources to a dozen offshore subcontractors, with the largest one in Thailand.

Although there are bills pending in several states that would prohibit overseas outsourcing, one would be apt to think that such would be ripe for federal legislation, yet

so far there has been little attention given these issues in either the 108th Congress or the present 109th Congress. Congressman Edward Markey (D-MA) recently appealed to the Internal Revenue Service to hold the tax return preparer responsible when a foreign person hired by a U.S. firm violates the protections which restrict unauthorized disclosure or misuse of personal information as contained in Sections 6713 and 7216 of the Internal Revenue Code. And Senator Hillary Rodham Clinton (D-NY) is calling for federal legislation which gives the “patient the right to know” that x-rays or other private healthcare information are being outsourced to countries outside of the U.S.

With offshoring by the U.S. showing no signs of slowing down in the near future, and with no “safe harbor” requirements in existing law offshore, it remains extremely difficult to prosecute security breaches within the confines of the U.S. justice system. Approximately 85 percent of U.S. critical infrastructure is owned by private, non-government businesses which have some component of their business being outsourced, admittedly with focus on profits and losses more of a priority than homeland security for these companies. In this respect lawmakers are behind the curve in protecting the interests of Americans. Yet it behooves and is incumbent upon the U.S. government, the legal community and privately held entities to join together in order to mandate protection for the best interests of the U.S and preserve the identities and economic health of the American people.

###

*Diane M. Grassi is a freelance columnist writing commentary on current events of the day providing honest and often politically incorrect assessments. From U.S. public policy to Major League Baseball, Ms. Grassi is an eclectic thinker, demanding the readers to also observe their thinking patterns from a different perspective. Whether you agree with her or not, Diane Grassi will have you coming back to note her opinions, and if at best she wakes you up, then her goal will have been accomplished.*

[dgrassi@cox.net](mailto:dgrassi@cox.net)

