

Client-Confidentiality may be compromised when traveling in U.S., says technology consultant

March 26, 2008, Miami, FL, USA: Businessmen in offshore financial centers and elsewhere who value client-confidentiality ought to think long and hard before taking laptop computers and other data-storage devices with them on trips to the United States, says Washington, DC-based technology consultant Mark D. Rasch.

There has been a growing number of incidents of travelers having electronic devices seized at U. S. airports by Government agents wanting to access the information stored on them, even if it is password-protected, according to Rasch, who is a former head of the U. S. Justice Department's computer crime unit, and now specializes in computer crime, computer security, incident response, forensics and privacy matters as Managing Director of Technology for FTI Consulting, Inc.

"People, money and information all travel across borders. Internet and computer technologies help facilitate the transfer of both information and money," he told OffshoreAlert. "However, despite the "borderless" nature of the Internet, real nations maintain real borders. In the United States and other countries, border patrol, customs and immigration officials have long maintained the right to inspect luggage coming into and out of the country.

"However, business travelers have recently learned that not only luggage is subject to inspection, but the contents of laptop computers, BlackBerrys, MP3 players, or other digital media are available for inspection.

"Customs agents have been pulling aside travelers, sometimes based upon some "profile," sometimes based upon "suspicion" and sometimes randomly, and inspecting computers for child pornography or other contraband. In addition, government officials reserve the right to copy the entire contents of hard drives, and to use the contents of these hard drives in any way they wish.

"Tax records, financial records, attorney client privileged information, or other personal data may be subject to inspection and use by the government, without any probable cause, warrant, or even suspicion."

Legally, it seems that Government agents "can do whatever they want" when it comes to snooping through your belongings at airports, says Rasch. "The computer is no different from any other "closed container" that the agent may search," he says. "Just as the agent needs no probable cause to search your underwear, they need no probable cause to rummage through your laptop. And besides, they are doing it to protect the country and enforce the laws and prevent terrorist attacks. You don't have any privacy rights at the border." Rasch's advice is simple. "If you don't want your laptop or BlackBerry searched, don't bring it with you."

His comments come after an article headlined 'Clarity Sought on Electronics Searches, U.S. Agents Seize Travelers' Devices' was published by the Washington Post newspaper on February 7, 2008. In the article, the newspaper documented

several examples of travelers having their laptops and other devices seized at U. S. airports and of Government agents asking for passwords to access information.

"The seizure of electronics at U.S. borders has prompted protests from travelers who say they now weigh the risk of traveling with sensitive or personal information on their laptops, cameras or cellphones," reported the newspaper. "In some cases, companies have altered their policies to require employees to safeguard corporate secrets by clearing laptop hard drives before international travel."

Recent data-leaking scandals such as client-account records of Julius Baer (Cayman) being uploaded to the whistle-blower's web-site Wikileaks, apparently by a former Chief Operating Officer, and the purchase by various tax authorities of stolen client data belonging to LGT Bank in Liechtenstein have thrust the issue of protecting client-confidentiality in the modern world to the forefront of business considerations, says Rasch.