MANY SLEEPLESS NIGHTS

10 Facts a Cloud-Based BSA/AML/Anti-Fraud Vendor Won't Tell You

The case of leaked secret documents in June 2013 by Edward Snowden – a young American citizen born on June 21, 1983 – has triggered a worldwide debate over whether the U.S. government should monitor civilians. Although an official statistic is not available, a comprehensive survey shows that a high percentage of U.S. citizens and an even higher percentage of foreigners support Edward Snowden. Many people even view Edward Snowden as a hero. The U.S. government takes the position that monitoring civilians is legitimate and Snowden should be brought back to the U.S. for indictment. However, the U.S. government has limited power to forbid foreigners from helping Snowden. As regulatory compliance professionals, we have learned some very important lessons from this case.

Snowden was not an employee of the National Security Agency (N.S.A.). Rather, Snowden worked for a contractor of the N.S.A. Each employee of the N.S.A. must go through a rigorous hiring process and intensive psychological evaluation and training. In contrast, Snowden did not have to go through these processes. Two very different standards are applied to employees of two different organizations.

The Snowden case highlights a serious problem for those financial institutions that use a third-party data center (i.e., the "cloud") to store their data associated with Suspicious Activity Reports (SARs). According to the Bank Secrecy Act (BSA), SAR data should be kept "secret" – a much higher standard than "confidential" which is required by the Gramm-Leach-Bliley Act regarding nonpublic personal data. Even a federal judge presiding on a legal case cannot see SAR data related to the case, but he can see any confidential data, including nonpublic personal data. Moreover, BSA/AML professionals have been carefully selected and well trained by financial institutions, while employees of a cloud vendor do not need to meet the same standards. Most importantly, a high percentage of people are Snowden supporters and it only takes one employee of a cloud vendor to leak SAR data to the public. The situation is even worse when the cloud vendor is a foreign company. When SAR data is stolen and published on the Internet, the following repercussions have been known to occur:

- Retaliation from suspected criminals reported in the SARs
- Severe reputational damage to the financial institution
- Career damage to the Senior Managers, BSA Officer, Compliance Officer, Security Officer, and Internal Auditor
- Countless trouble with government agencies
- Loss of shareholder confidence in the financial institution's management team

In addition, WikiLeaks and many hackers are very interested in hacking cloud databases, which store concentrated SAR data from many financial institutions. In fact, cyber-attacks are a major concern to government regulators, which have emphasized that the reliance of a financial institution on the cloud will make the financial institution more vulnerable to hackers. **Here are 10 facts that a**

GlobalVision Systems, Inc. 9401 Oakdale Avenue, Chatsworth, California 91311 • www.gv-systems.com

BSA/AML/Anti-Fraud vendor won't tell you before it keeps your SAR data in the cloud (i.e., a third-party data center):

1. Employees of a cloud vendor can easily steal your secret SAR data just as Snowden did to the N.S.A.
2. The cloud is an easy target for WikiLeaks and many hackers around the world.
3. SAR Data should not be accessible to foreign companies or persons who are not under U.S. jurisdiction.
4. Keeping your SAR data with a cloud vendor, which is a subcontractor of your BSA/AML vendor, will double your risk exposure because employees of both vendors can easily steal your SAR data.
5. Single sign-on is very important to financial institutions. However, single sign-on is not possible if the system is hosted in the cloud.
6. It is impossible for a cloud vendor to timely prevent fraud for your financial institution because the cloud vendor cannot move all data from different systems (e.g., wires, ACH, credit card, debit card, Internet Banking, etc.) to a cloud computer in real-time.
7. Your financial institution is liable for the decision of sending data from your core system to the cloud through the Internet where hackers can easily steal the data.
8. It raises many compliance problems to ensure that your financial institution meets industry standards such as PCI compliance, etc. when your data is kept by a cloud vendor.
9. Your BSA/AML and Anti-Fraud System in the cloud can be affected by activities of many other companies, which use the same cloud. Similar to sharing a road with many cars, traffic jams may frequently occur at any time. Moreover, if one car breaks down, other cars will come to a halt.
10. When you try to end your relationship with a cloud vendor, the cloud vendor can hold your SAR data hostage until you pay money to get your SAR data back.

In summary, keeping data in the cloud may be acceptable to Google, Facebook, etc. because these companies do not have SAR data that is classified as "secret" by the U.S. Government. Additionally, these companies are not tightly regulated like financial institutions. The Snowden case has given Financial Institutions, Board Directors, Senior Managers, BSA Officers, Compliance Officers, Security Officers, and Internal Auditors an alarming omen that **moving SAR data to the cloud will be the beginning of many sleepless nights**.

Publisher Background

GlobalVision Systems, Inc. is the largest independent provider of regulatory compliance, risk management and fraud prevention solutions in the U.S.A. It has produced the renowned PATRIOT OFFICER®, GUARDIAN OFFICER®, and ENQUIRER OFFICER® and has established the de facto standards for BSA/AML compliance in the USA. For more information, please contact sales@gv-systems.com or (888) 227-7967.

GlobalVision Systems, Inc. 9401 Oakdale Avenue, Chatsworth, California 91311 • www.gv-systems.com