LOST SAFE HARBOR

Are you truly protected by the Safe Harbor of Section 314(b)?

Two interesting questions have been raised recently regarding (1) whether a financial institution can legally search the confidential customer databases of other financial institutions on the same cloud, based on Section 314(b) of the USA PATRIOT Act, and (2) whether Section 314(b) of the USA PATRIOT Act can be applied for fraud prevention purposes. Both answers are "No."

It is obvious that "information sharing" has a different meaning from "database search." Although Section 314(b) of the USA PATRIOT Act provides a Safe Harbor for financial institutions to share information for ***anti-money laundering and counter terrorist financing*** purposes (not for fraud prevention), such Safe Harbor has very strict limitations listed in paragraph (b)(5) of 31 CFR 1010.540 (the "Section") as shown below:

> (b)(5) Safe Harbor from certain liability
>
> (i) In general. A financial institution or association of financial institutions that shares information pursuant to paragraph (b) of this Section shall be protected from liability for such sharing, or for any failure to provide notice of such sharing, to an individual, entity, or organization that is identified in such sharing, to the full extent provided in subsection 314(b) of Public Law 107-56.
>
> (ii) Limitation. Paragraph (b)(5)(i) of this Section **shall not apply** to a financial institution or association of financial institutions to the extent such institution or association **fails to comply with paragraphs (b)(2), (b)(3), or (b)(4) of this section**.

For your reference, paragraph (b)(2) of the Section requires a participant of the information sharing activity to submit a notice to FinCEN first and each notice has an effective period of only one year. If the participant intends to continuously share information, the participant must file a notice again when the prior notice expires. Paragraph (b)(3) of the Section requires the participant to ensure that the counter party of the information sharing activity has also met the requirement of paragraph (b)(2) before sharing any information. Paragraph (b)(4) of the Section requires that the information received from the information sharing activity only be used for anti-money laundering and counter terrorists financing purposes and the received information be kept confidential.

Therefore, **Safe Harbor protection can be lost and the financial institutions may be exposed to huge liabilities if there is a failure to distinguish between "information sharing" and "database search."** If counter parties on the cloud (or the vendor) are allowed to search a financial institution's customer database, it is important to keep in mind the potential damages when any of the following incidents occurs:

- any counter party on the cloud has failed to correctly submit a notice to FinCEN because of human mistake, system mistake, negligence, misconduct of a disgruntled employee, or any other reason;
- any counter party on the cloud has failed to resubmit a notice on time every year due to any reason;

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

- any counter party on the cloud has used your data for purposes other than what is permitted by paragraph (b)(4);
- any counter party on the cloud has failed to keep your data confidential; or
- any employee or contractor of any counter party (or the vendor) gives your data to a fraudster.

A similar set of issues also apply when searching the databases of the counter parties on the cloud. When any counter party fails to fully comply with 31 CFR 1010.540, the financial institutions on the same cloud could lose the Safe Harbor protection.

Some vendors argue that money laundering always occur after fraud and detecting fraud is the same as detecting money laundering. This argument is false. For example, when a fraudster uses a victim's credit card to conduct a shopping spree, there is no money laundering activity at all. For most fraud cases detected by financial institutions, such as check fraud, credit card fraud, debit card fraud, ATM fraud, ACH fraud, wire fraud, etc., the customers in these fraud cases are "victims" of the fraud and they are not money launderers. The fraudsters are actually unknown and there is no money laundering activity that has occurred in the financial institutions. This is the reason why FinCEN's Suspicious Activity Report (SAR) form has clearly separated money laundering activity from fraud activity. More importantly, a responsible vendor should never provide any tool for another party to search a financial institution's customer database. It is risky to assume that all employees and contractors of all financial institutions on the cloud are trustworthy. If a financial institution allows any party to search its database and the data is compromised, **the financial institution may be liable for gross negligence, intentional misconduct, and punitive damages.** The financial institution may also be reported by whistleblowers who can receive substantial monetary rewards based on the Dodd-Frank Act.

When choosing a vendor, financial institutions are responsible for being compliant with 31 CFR 1010.540 or any other laws and regulations. It is also important to know that customers can file lawsuits against the financial institution if the Safe Harbor protection is lost.

In summary, because it is impossible that all parties on the cloud will comply with all the applicable regulations and laws all the time, issues may arise regarding Safe Harbor protection provided by Section 314(b). Issues related to the Gramm-Leach-Bliley Act, the USA PATRIOT Act, and other applicable laws and regulations may also arise. Furthermore, Section 314(b) cannot be applied for fraud prevention purposes. The Dodd-Frank whistleblowers are highly motivated. The regulatory penalties are huge and the lawsuits are expensive these days. It is important that due diligence is conducted to fully understand Safe Harbor protection with regard to any vendor.

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