REJECTED BY SAFE HARBOR

The Beginning of Endless Lawsuits and Regulatory Penalties

Two important questions have been raised recently regarding **(1) whether a financial institution can post its customer (or member) information on a website 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.**

In fact, FinCEN has specifically stated: "An entity that participates in the 314(b) program and that fails to maintain appropriate procedures to ensure compliance with the requirements stated in 31 CFR § 1010.540(b) may be subject to penalties."

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, it cannot be used for fraud prevention purposes**. The 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 terrorist financing** purposes and the received information be kept confidential.

Therefore, **all the financial institutions on the website may lose the Safe Harbor protection if any of the following incidents occurs**:

- any person fails to correctly submit a notice to FinCEN because of human mistake, system mistake, negligence, misconduct of a disgruntled employee, or any other reasons;
- any person fails to resubmit a notice on time every year due to any reasons;
- any person, who posted information on the website before, decides not to renew its 314(b) status with FinCEN anymore for whatever reasons;
- any person uses the information posted on the website for fraud prevention purposes; or
- any person (or the vendor) fails to keep the data of the website confidential; etc.

It is also important to know that customers (or members) can file lawsuits against the financial institution if the financial institution loses 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, etc., the customers (or members) 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 website for financial institutions to post customers' (or members') information. **If any person on the website violates any part of 31 CFR 1010.540(b), all the financial institutions on the website may be liable for gross negligence, intentional misconduct, and punitive damages.** The financial institutions which use such website may also be reported by whistleblowers who can receive substantial monetary rewards based on the Dodd-Frank Act.

In summary, because it is impossible that all parties, who either post or use the information on a website, will fully comply with 31 CFR 1010.540(b) all the time, all financial institutions on the website may lose the Safe Harbor protection provided by Section 314(b). **Violations** of the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Bank Secrecy Act, etc. **are doomed to happen**. FinCEN has also repeatedly warned that 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. **To protect yourself and your financial institution, tell your team members that they should immediately remove all the customer (or member) information they have ever posted on any websites and they should never go to those websites again.**