PUBLICATION

Issues to Consider When Retaining Third-Party Vendors for CTA Filing Services

Authors: David J. Oberly
October 03, 2024

The Corporate Transparency Act (CTA) requires many companies formed or registered to do business in the U.S., to file extensive beneficial ownership information to the Financial Crimes Enforcement Network (FinCEN) no later than January 1, 2025. With the compliance deadline fast approaching, many businesses are evaluating their options as to how they can most effectively and efficiently satisfy their CTA filing obligations.

A significant portion of those organizations that have yet to submit their CTA filings to FinCEN are likely considering the option of relying on one of the many third-party CTA filing services that can streamline the CTA filing process. Importantly, however, even minor CTA noncompliance can result in significant civil monetary penalties, as well as criminal ones – including *imprisonment.* With so much at stake, companies must ensure that any retained vendor possesses the capabilities and personnel necessary to ensure all CTA obligations are satisfied in a compliant and timely manner.

Companies that use third-party vendors for CTA filing will be required to input personal data about beneficial owners into the vendor's portal or other systems, sometimes for future storage as well. Those companies need to be cognizant of the patchwork of global laws and regulations governing the handling and safeguarding of personal data, which place strict requirements and restrictions on how their organizations can collect, use, and disclose/transfer such data. This, in turn, creates expansive legal risk and liability exposure for all types of third-party vendor relationships, which are broadened by a considerable margin due to the fact that cyberattacks directed at vendors remain prevalent in terms of their frequency, severity, and cost.

Companies should take proactive steps to address and mitigate these outsized risks in connection with any prospective vendors who may process or otherwise have access to organizational personal data. In particular, before entering into any contractual relationship, companies should conduct thorough diligence and vetting of vendors to identify potential risks and ensure collaboration with only those vendors who are committed to protecting the company's business, brand, and customers, as well as to strict legal and regulatory compliance. Through systematic vetting, companies can avoid retaining vendors who fail to meet organizational compliance and security needs and expectations.

Key Considerations

As indicated above, two significant risks that companies must address during the vetting process are: (1) security risks, which arise from a vendor's deficient or missing security controls; and (2) legal and regulatory compliance risks, which arise from a vendor's failure to comply with applicable laws and regulations governing how it must handle personal data when supplying its services and solutions to customers. The following are key areas of vetting that should be addressed when conducting diligence on prospective vendors:

1. Security and incident response programs. Companies should evaluate prospective vendors' security and incident response policies and practices, including: (1) whether the vendor has a formal information security policy that is regularly reviewed and updated as needed; (2) the technical security controls used by the vendor,

such as firewalls and multifactor authentication; and (3) whether the vendor has a dedicated incident response plan that includes defined procedures pertaining to rapid response, disaster recovery, and business continuity.

2. Security certifications. Companies should ascertain whether prospective vendors hold any certifications with recognized security frameworks and standards. ISO/IEC 270001 is the most universally recognized standard for information security management systems. Conformity with ISO/IEC 27001 means that a vendor has put in place a system to manage risks related to the security of data owned or handled by the vendor and that the vendor's system adheres to all best practices and principles enshrined in this international standard. Systems and Organization Controls 2 (SOC 2) is another widely recognized certification that is relevant for evaluating and validating prospective vendors' information security practices. Conformity with SOC 2 means that a vendor's security program meets defined criteria for managing personal data based on five "trust service principles" – security, availability processing, integrity, confidentiality, and privacy.

3. Security incident history. Companies should evaluate whether prospective vendors have experienced any prior security incidents or other data compromise events. If so, further investigation should be completed to determine whether the vulnerabilities leading to such incidents or events have been identified, addressed, and remediated.

4. Legal and regulatory compliance program. Companies should verify that prospective vendors have in place an enterprise-wide compliance program to facilitate ongoing, continued compliance with applicable privacy and security laws and regulations, as vendor compliance mishaps can result in significant liability for companies, even where the vendor is exclusively responsible for such legal or regulatory violations relating to the services or solutions provided to the company.

5. Legal and regulatory noncompliance history. Companies should also ascertain the existence of any complaints, claims, demands, subpoenas, regulatory investigations or enforcement actions, or litigation involving the vendor and resulting from its non-compliance with applicable privacy and security laws and regulations. If so, further investigation should be completed to determine whether any such matters remain pending and unresolved and whether the vendor has taken steps to remediate any deficiencies that gave rise to those matters.

6. Personnel vetting and training. Companies should determine whether prospective vendors conduct background checks on their personnel who may be responsible for processing or may otherwise have access to, customer personal data. Companies should also evaluate the nature and extent of prospective vendors' internal education and training programs, especially as it relates to the extent to which such programs address relevant vendor legal/regulatory obligations and risk management best practices.

Conducting Vendor Diligence and Vetting

There are several methods through which companies can conduct prospective vendor diligence and vetting, including the following.

1. Written questionnaires. Companies can develop and implement a standardized, written questionnaire for prospective vendors to complete that addresses the issues identified above, as well as any other company-specific risks or needs. Written questionnaires provide companies with significant visibility into prospective vendors' compliance programs, as well as their security posture and practices.

2. Site visits. Companies can supplement their written questionnaires with site visits to validate and confirm a prospective vendor's written responses and supporting documentation. Site visits allow companies to evaluate

– in real-time – whether and how prospective vendors have implemented their security practices and protocols, such as physical access controls and data retention/destruction mechanisms, among others.

3. Audit reports. Companies can request prospective vendors' internal or external audit reports to further evaluate adherence to security industry best practices, and the level of compliance with applicable laws and regulations. Audit reports provide an added layer of assurance that prospective vendors have the necessary practices and protocols in place to effectively address relevant compliance and security risks. In addition, oftentimes audit reports will include information pertaining to identified security vulnerabilities or deficiencies, and whether those risks have been fully remediated.

4. Ongoing monitoring. Importantly, *after* selecting a vendor who will process organizational data or otherwise have access to such data, ongoing monitoring must continue throughout the duration of the contractual relationship. All vendors should be reviewed regularly, such as through written questionnaires. Higher-risk vendors, including those who process sensitive data, should be subject to a more thorough and exacting review, such as through third-party external audits (that must be conducted with the assistance of experienced outside counsel to ensure the audit is covered by the attorney-client privilege) to confirm ongoing legal/regulatory compliance and conformity with security-related industry best practices.

The Final Word

In our highly digital world, reliance on outside vendors and other third-party support services will continue to increase moving forward. At the same time, applicable third-party legal risks and liability exposure will likewise continue to expand. Taken together, companies must ensure they maintain effective, comprehensive third-party risk management programs that include, among other things, diligence and vetting protocols – which can play a vital role in managing and mitigating the risk of retaining vendors who may fail to meet organizational compliance and security needs and expectations. For more information on this topic, please contact one of the following people: David J. Oberly, Mary Ann Jackson, or Perry F. Sofferman, or visit Baker Donelson's Corporate Transparency Act webpage