ROETZEL
FOCUSED ON WHAT MATTERS TO YOU

CORPORATE COMPLIANCE ALERT

5/15/15

Identity Theft through Breach of Third-Party Vendor Systems on the Rise

Many companies outsource portions of their business activity to outside vendors, including tasks such as payroll, mail-order or online purchasing, credit card processing, and a multitude of other functions. However, third-party vendors are an increasingly common source of data security breaches, as one Roetzel client recently found out to its detriment when it was notified that its employees' personal identification and tax information was stolen via a breach of their payroll processing company's systems. The identity thief used the stolen personal identification information to file fraudulent tax returns on behalf of several employees. Identity thieves will always follow the path of least resistance, which is why it is vital for companies to ensure not just the security of the IT systems that they personally oversee and control, but to verify that their vendors employ stringent cybersecurity controls as well.

Companies contracted with third-party vendors whose tasks will put them on the target list for potential hackers should undertake a due diligence process that assesses the cybersecurity controls in place to protect the information that flows between the two parties. Some of the considerations in this process include an assessment of the vendor's

- Physical security, firewall protection, and malware, anti-spam, and antivirus protection and detection;
- Software applications in use;
- Protection and encryption of laptops and wireless devices;
- Cybersecurity documentation and training of personnel; and
- Procedures in the event of a data breach.

Companies should also review insurance policies and third-party vendor contracts regarding data breach protection and policies.

Conducting the assessment up-front and before any contract is signed is the ideal, but even in the case of an existing contract, a regular review of a third-party vendor's cybersecurity is warranted. A company should engage its own IT security professionals to coordinate with the company's legal team to make sure compliance and cybersecurity concerns are met, rather than relying on a "check the box" verification from a vendor. Writing the requirements and protocol into the contract is also necessary. A third-party vendor with its own, let alone a partner's, best interests at top of mind should always be ready and willing to mitigate risk when it comes to cybersecurity.

Cybersecurity, like other corporate compliance areas, is best served through proactive assessment of risks – both internal and external. Please contact any of Roetzel's Corporate Compliance team for further information on the implementation or assessment of a cybersecurity plan.

Brian E. Dickerson
Practice Group Manager
White Collar Litigation & Corporate Compliance
202.570.0248 | bdickerson@ralaw.com

Anthony J. Calamunci
419.254.5247 | acalamunci@ralaw.com

James L. Ervin, Jr.
614.723.2081 | jervin@ralaw.com

Amanda M. Knapp
216.615.7416 | aknapp@ralaw.com

Thomas M. Larned
202.697.4892 | tlarned@ralaw.com

Nicole Hughes Waid
202.906.9572 | nwaid@ralaw.com