TIPS FOR PROTECTING CLIENT DATA & MINIMIZING LIABILITY FOR CYBERATTACKS

BY MAUREEN FULTON & MIKAELA WITHERSPOON, KOLEY JESSEN

THE SURGE IN NEW STATE DATA PRIVACY LAWS HAS LEFT MANY service providers concerned about potential regulatory enforcement and fines in the event that data they control is subject to a breach event. As a result, the security of personal data and resulting liability in the event of a data breach is quickly becoming a major component of many commercial contracts as service providers face potential liability for cyberattacks that compromise third-party and customer data. This is an especially pressing concern given the increasing frequency and complexity of cyberattacks in the private sector.

CPA firms can be compelling targets for cybercriminals due to their extensive collection of clients' personal information, such as Social Security numbers, addresses, phone numbers, and financial information. The compromise of personal information and the resulting lawsuits, legal fees, and settlements or fines may result in exorbitant damages that could threaten the commercial existence of a firm. CPA firms can distinguish themselves from competitors by staying up to date with requirements under relevant data privacy laws and regulations and maintaining strong privacy and cybersecurity systems.

As financial institutions that are "significantly engaged" in providing financial services or products, CPAs are subject to the Gramm-Leach-Bliley Act (GLBA) and are required to establish measures to keep clients' nonpublic personal information secure.[i] Failure to comply with the requirements of the GLBA can have serious consequences, with a financial institution that violates the GLBA facing fines of up to $100,000 per violation.[ii]

In addition, recent developments in state data privacy laws may make some information held by CPAs subject to further legal obligations. The GLBA preempts state laws only to the extent that a state law is "inconsistent" with the requirements of the GLBA. If a state law provides greater protection for consumers than the GLBA, it is not "inconsistent" with the GLBA and the state law will also apply. The California Consumer Privacy Act (CCPA) and Virginia Consumer Data Protection Act (VCDPA), the only two state data privacy laws currently in effect, apply in conjunction with the GLBA, but do contain some exemptions applicable to CPAs.

The CCPA includes a partial exemption for information collected by financial institutions where the information is "subject to" the GLBA. Information subject to the GLBA is exempt from the requirements of the CCPA, other than the private right of action for consumers related to a data breach. However, information collected by a financial institution that is not "subject to" the GLBA remains subject to all CCPA requirements.

The VCDPA contains a full exemption for financial institutions and their affiliates that are subject to the GLBA. The three additional state privacy laws coming into effect later in 2023 also contain exemptions for financial institutions subject to the GLBA.[iii]

Service providers have three key opportunities to protect their clients' data: internal operating procedures, security requirements for clients, and insurance coverage.

i https://www.aicpa.org/professional-insights/article/cpa-cyber-obligations-and-breach-response
ii https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act
iii The Colorado Privacy Act and the Connecticut Data Privacy Act become effective on July 1, 2023, and the Utah Consumer Privacy Act becomes effective on December 31, 2023.

Internal Operating Procedures

Adopting formal operating procedures for managing security risks is highly advisable, and may even be contractually required in some instances. CPA firms should consider developing centralized guidance containing all data security-related actions that must be taken pursuant to agreements with customers and with their own vendors, including specific firewall requirements or user authentication systems. These requirements should be reviewed prior to any changes to the firm's IT and security systems to ensure any update does not inadvertently put the provider in breach of an agreement. This document should also summarize the substantive contractual requirements related to a data breach, such as the time for notice to the other party and any indemnification obligations for the firm. A similar approach should be taken with regard to keeping track of all duties imposed by federal, state, and local laws and regulations, as well as relevant case law developments that have an impact on those duties.

CPAs should also keep a record of internal plans regarding data breaches, making sure to build out contingency plans for various types of breaches. These plans should involve any legal or public relations response that the firm may need to undertake. Consulting with legal counsel is highly recommended in developing these plans, as such plans must take account of rapid changes in privacy and data security law and should be developed with an eye towards potential future litigation.

Imposing Security Requirements on the Customer

CPA firms should seek to impose security requirements on the customer when the services will require the firm to access the customer's system, or when the customer will have some access to the firm's own system. For example, a firm might obligate customers to shore up the security of their technology ecosystems by mandating maintenance of firewalls or network access protocols. This language should be carefully constructed to prevent developments in technology and cyber threats from rendering it obsolete. One way to accomplish this is to reference accepted industry cybersecurity standards, such as the U.S. Department of Commerce NIST framework.

If service providers decide to include these kind of requirements in their contracts, they would be well advised to treat and contractually require their customers to treat them as strictly confidential. Knowledge of a service provider's security protocols can be useful to malicious actors attempting to breach the service provider's system or service.

Insurance Coverage

CPA firms should ensure they have proper insurance coverage for data breach liability. Many commercial general liability insurance policies contain exclusions for cyberattacks and related issues. Some insurers will not cover data breach liability, while others will only do so if an insured purchases the correct endorsement. Firms should seek out cyber coverage that will pay the costs of investigating potential breaches, providing affected parties with notice of breaches, and paying employees for additional time and effort required to respond to breaches. Such coverage may also pay for the costs of data restoration, blackmail or extortion, loss of business income, and legal fees that arise out of data breaches.

Protecting clients' data is not only a legal obligation but is also critical for maintaining trust and credibility, making robust data security measures essential. Utilizing these three key opportunities to safeguard your clients' personal information and ensuring data security can help you minimize liability of cyberattacks. ◀

Maureen Fulton is chairman of Koley Jessen's Data Privacy and Security practice. She advises businesses on developing comprehensive privacy and data security programs and provides guidance to companies as they navigate through state, federal, and international privacy laws and regulations. Fulton has supported numerous clients in preparing for and responding to data breach incidents and also has extensive experience in performing data privacy and security due diligence for buyers and sellers in merger and acquisition transactions. She can be reached at maureen.fulton@koleyjessen.com.

Mikaela Witherspoon is a staff attorney with Koley Jessen. She counsels clients on various data privacy matters, including compliance with privacy laws such as the EU's GDPR and California's CCPA. With her knowledge of the interplay of intellectual property, data privacy, and commercial law, Witherspoon also drafts and reviews data transfer, data license, and software license agreements, as well as other technology-related contracts that protect clients' rights and intellectual property, while also minimizing liability and ensuring compliance with privacy and data protection regulations. She can be reached at mikaela.witherspoon@koleyjessen.com.

SECTION 1031 EXCHANGE

IPE 1031 QUALIFIED INTERMEDIARY SERVICES

THE PREMIER SPECIALIST FOR SECTION 1031 EXCHANGES

EXPERTISE

From a Respected Industry Leader

FEA FEDERATION OF EXCHANGE ACCOMMODATORS

CES 1031 Certified Exchange Specialist on Staff

IPE 1031 | 888.226.0400 |
WWW.IPE1031.COM | INFO@IPE1031.COM