Pennsylvania Institute of Certified Public Accountants
(PICPA)
Testimony
to
Pennsylvania House Commerce Committee
February 25, 2020
On behalf of the Pennsylvania Institute of Certified Public Accountants (PICPA), thank you for the opportunity to discuss House Bill 1010 and the broader issue of data privacy.

The PICPA, founded in 1897, is the second-oldest and the fourth-largest CPA organization in the United States. Membership includes more than 20,000 practitioners in public accounting, industry, government, and education. One of our expressed goals is to speak on behalf of members when such action is in the best interest of the CPA profession in Pennsylvania and the public interest.

Every tax professional in the United States -- be they a member of a major accounting firm or an owner of a one-person storefront -- is a potential target for highly sophisticated, well-funded, and technologically adept cybercriminals around the world. Their objective is to steal client data in order to file fraudulent tax returns that better impersonate their victims and are more difficult to detect. In addition, fraudsters are seeking access to information to open credit cards or take out loans under the identity theft victims’ names.

Protecting client data is already the law and a priority for tax professionals. The Federal Trade Commission’s (FTC) “Safeguards Rules” require professional tax preparers to create and enact security plans to protect client data. Additionally, the IRS may treat a violation of the FTC’s Safeguards Rules as a violation of IRS Revenue Procedure 2007-40, a provision which sets the rules for tax professionals participating as Authorized IRS e-file Providers. Treasury regulation section 301.7216, and recently released Revenue Procedure 2008-35, also provide a complete authoritative guidance on the disclosure or use of tax return information. Section 7216 of the regulation prohibits tax return preparers from “knowingly or recklessly” disclosing or using tax return information. As a criminal provision, this section could result in the preparer being charged with a misdemeanor, involving a maximum penalty of $1,000 or one year in prison, or both, plus costs of prosecution. Lastly, tax professionals are also required to abide by the Gramm-Leach-Bliley Act, also known as the Financial Modernization Act of 1999. It is a U.S. federal law that requires financial institutions to explain how they share and protect their customers' private information. Certified public accountants must abide by these various standards because of the sensitive nature of the information required to do their job which in turn makes them prime targets for various types of cybercrime and identity theft.

Enhanced data privacy seems to be the wave of the future for all professions that handle sensitive information. For example, at least nine other states have introduced data privacy bills to protect individuals and the professions that are most at risk for attacks. Ohio has a voluntary data protection law in place offering civil protection that first looks to federal or state regulation, then the PCI-DSS (Payment Card Industry-Data Security Standard), and lastly Industry recognized cybersecurity frameworks. Ohio’s law provides incentive for businesses to achieve a higher level of cyber security through voluntary action. If a business has a cybersecurity program that meets one of the acts requirements, it is eligible to use affirmative defense in the event of a lawsuit resulting from a data breach. Additionally, California is preparing to implement its Consumer Privacy Act (CCPA), a data privacy law that is among the strictest in the country. California’s law is similar, but not identical, to the European Union’s General Data Protection Regulation (GDPR)
that took effect in 2018. California’s consumer privacy act, could have major repercussions on U.S. companies as it is not totally clear what it means to be compliant, leaving many companies in a struggle to interpret grey areas created by the law. It is common practice for CPA firms to employ general counsel or a lawyer to ensure that they are in compliance with the various standards that are in place and that they are prepared to take the proper recourse should a data breach occur.

In addition to accountants being targeted because they are in possession of taxpayer and other client data required to comply with tax filing, cybersecurity concerns also touch the services offered by many CPA firms. Some perform attestation engagements in the realm of third-party information processors (System and Organization Controls Report), so the profession is acutely aware of the reporting and liability issues that arise from cybersecurity from the perspective of providing services for companies whose data can be breached. Additionally, many CPAs/CPA firms obtain accounting data files for small businesses that contain vendor details including ID numbers and the confidential information of independent contractors for which annual 1099s are prepared, and payroll details for employees and business clients, potentially providing for many more ID theft victims.

A number of CPA firms are national and international firms. One state statute can alter protocols nationwide for some, which may pose a significant cost to firms above and beyond the potential for penalties associated with data breaches for Pennsylvania residents. While most CPA firms are prepared to adhere to the federal laws in place should a data breach occur, the penalty formula outlined in Pennsylvania House Bill 1010 is overburdening and has the potential to put firms out of business, ultimately resulting in a loss of jobs due to overregulation. For example, if a CPA prepared a return for a married couple with four children, the minimum penalty for the breach of just one return could be six times the $5,000 individual penalty, or $30,000. Not to mention, this legislation allows the Attorney General to issue a $10,000 penalty against anyone who violates this act. That cost is in addition to all the other breach remediation costs incurred – which often range well into the thousands. Furthermore, malpractice premiums will skyrocket under a $5,000 per person penalty. The potential cost to obtain expanded liability coverage to help mitigate the exposure presented by this legislation could likely spike malpractice professional liability insurance 200%, 300% or more -- a cost many small businesses will not be able to afford.

CPA firms also represent many for-profit and not-for-profit clients who may view the proposed House Bill 1010 as a serious threat to their ongoing viability if they are exposed to substantial automatic monetary damages. Entities covered by HIPPA (Health Insurance Portability and Accountability Act), FERPA (Family Educational Rights and Privacy Act), and similar regulatory regimes regarding privacy may be affected differently by the proposed statute. The ongoing growth of automation technology affects the profession as well. Artificial intelligence (AI) programs and data analytics may expose CPA firms to additional risk because AI systems and data analyses performed in attest and consulting businesses may contain the data of a client's customers, employees, and vendors, not just data about the client.
Ultimately, CPA firms and businesses housing sensitive data are tasked with performing due diligence and maintaining adequate coverage. This would include having knowledge of the threats they face, common regulatory requirements they must adhere to – both state and federal laws – and having an understanding of cyber insurance policy specifics.

It is a nightmare for CPAs, especially tax practitioners, when a hacker gains access to sensitive client data and files fraudulent returns. Susan Jarvis, CPA, learned this firsthand during the 2017 tax filing season. Jarvis, a responsible small-business owner, was already taking all the precautions required to protect her firm and her clients. She had done her due diligence, employing an external IT firm who was constantly monitoring her system in addition to having various firewalls in place. As it turns out, Jarvis became a victim when a hacker accessed her company’s system through her staff member’s remote location. The forensic team informed Jarvis that hackers typically have access to a system for an average of 210 days, (7 months) before one knows a breach has occurred.

After becoming aware of the breach, Jarvis immediately notified clients, a step she indicated as crucial, as clients will also receive notification from the IRS. One could infer that it is in a company’s best interest to notify clients immediately, otherwise they will be blindsided. She was extremely diligent throughout all stages of the process. In total the breach ended up costing around $26,000 – which Jarvis describes as minimal. Larger firms could incur costs amounting to hundreds of thousands of dollars. Jarvis indicated that had the state assessed the type of penalty outlined in House Bill 1010, she would not be in business today.

From this personal experience you can see how a responsible business owner fell victim to a nightmare scenario despite having several measures in place to ensure her clients’ information was protected. No one is immune to cyberattacks, nor can their timing be predicted, especially in a world where it is common to conduct business virtually. The stakes are high, and the implications are real for CPA firms and their clients. We are committed to working with the state legislature to ensure that the personal information of Pennsylvanians is secure and hope to be a resource as you work to enhance policies to better protect individuals and businesses.

The PICPA is happy to serve as a resource and will be glad to answer any follow-up questions. Thank you for the opportunity to provide testimony.