CASE STUDY

TaxSlayer protects consumer information from inadvertent disclosure as 500 staff members shift to work from home within 48-hours of a statewide mandate

"TaxSlayer was securely and confidently able to move their staff to work from home within 48 hours of the shelter-in-place order, while the Spirion agent helps protect the organization from inadvertent disclosures."

Michael Blache, Chief Information Security Officer, TaxSlayer

About the Customer

TaxSlayer® LLC is a privately held tax preparation and financial technology company based in Augusta, Georgia. The company offers online tax preparation technology for American consumers and tax professionals, allowing them to electronically file state and/or federal returns.

Industry Challenge: Protect taxpayer data with vigilant security practices

Cybercriminals are always searching for weak links. These bad actors increasingly target tax professionals and taxpayers to steal valuable personal and financial information by using phishing emails, exploiting unsecured networks, or capitalizing on other weaknesses. Highly valuable taxpayer information can be used to create fraudulent tax returns and claim fake refunds. On April 14, 2020, the Internal Revenue Service (IRS) issued a warning urging tax professionals to "take additional security steps to protect taxpayer data as more practitioners telework and security risks increase."

The IRS news release advises tax professionals to remain vigilant and use an encrypted virtual private network (VPN) for teleworkers, adopt multi-factor authentication, remain aware of IRS impersonation scams, employ caution to avoid phishing scams, and to implement security software to protect client information.

The Need: Maintain business continuity and protect consumers personally identifiable information (PII) during the height of tax season and beyond

Both Michael Blache, TaxSlayer's CISO, and Ricky Bryant TaxSlayer's Director of Information Security, recognize the criticality of keeping their business secure by deploying robust data protection solutions, educating employees, and setting appropriate protocols. Given the sensitive nature of their business, TaxSlayer's® main objective is to be the first line of defense, ensuring that all customer tax filings are secure - from the point of entry, through processing, and to the data center. Both Blache and Bryant were confident Spirion's Sensitive Data Manager (SDM) could protect their customers' personal information.

TaxSlayer's primary concern was the presence of consumers' protected personally identifiable information (PII) on employee workstations. At the same time, TaxSlayer faced an internal challenge that they referred

© 2020 SPIRION, LLC. ALL RIGHTS RESERVED

to as the “Wild Wild West” project. Traditionally, TaxSlayer workstation access was limited to their private business network, but developers requested more flexibility. To accommodate, the technical team configured secure remote access.

The Solution: The most accurate data protection solution so employees can focus on business-critical work

Following a successful proof of concept (POC), TaxSlayer determined that Spirion’s solution was well suited for their needs and moved forward with procuring the solution. During the implementation of Spirion, Blache’s team was quickly able to discover, classify, and apply security controls to all personal data. One of the significant benefits TaxSlayer experienced during the testing and configuration of Spirion was that they were able to leverage Microsoft’s Azure Information Protection (AIP) solution to label the most sensitive data for increased protection.

Before Spirion, TaxSlayer actively evaluated several alternative solutions, but without finding the right technology for their needs. With other solutions, they experienced system performance, scalability, data search, productivity, and network impact challenges. TaxSlayer found SDM the most accurate and suitable solution for their environment. “Spirion provides the level of protection we need without negatively impacting productivity,” said Blache. “Employees used to complain about previous products that we tried to implement because they would disrupt their work. With Spirion, those complaints have dropped to zero. The endpoint agent is not in-your-face, and once it identifies sensitive data, it immediately acts on it. SDM keeps endpoints secure, which enables employees to focus on business-critical work.”

In addition to Microsoft AIP, TaxSlayer configured Spirion to work in conjunction with their third-party cloud-based proxy firewall to route all employee traffic through the solution. The TaxSlayer team applied policies based on their Zero Trust model to protect the network.

The Results: Zero Disruption During a Challenging Time

Spirion has helped TaxSlayer improve the accuracy of data discovery, reduce risk with data remediation, and ultimately improve the efficiency and speed associated with finding personal data. Even more, the investment in Spirion and the firewall, combined, cost less than their previous data discovery solution alone.

When the Coronavirus pandemic caused the United States and the rest of the world to shut down, TaxSlayer was forced to quickly transition their call center employees to a remote work model. Shutting down was not an option amid tax season, with millions of tax returns left to process. On April 2, Georgia Governor Brian Kemp issued a statewide shelter-in-place order, less than two weeks before the country’s annual tax filing deadline. Within 48-hours of the mandate, TaxSlayer transitioned its 300 seasonal call center staff and 200 permanent employees to work remotely. Having implemented Spirion before the state’s shelter-in-place order, TaxSlayer was confident that consumers’ personally identifiable information (PII) did not live on employee workstations, but instead, was secure in their data center. Seasonal tax specialists could work from home since each laptop was loaded with a Spirion agent, which either locked sensitive data down on the endpoint or remediated the information.

The TaxSlayer information security team reviews all suspicious data. Since the seasonal and permanent team moved to a remote work model, they have discovered only one instance of a full tax return on a computer, and fortunately, that was an employee preparing their own tax return.

Looking toward the future, TaxSlayer will continue working with Spirion to expand its auditing of personal data, as well as scanning structured data in their SQL databases to ensure that it is following their internal policies.

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion is the leader in data discovery, persistent classification, and protection of sensitive data on-premise and in the cloud. Since 2006, thousands of organizations worldwide have reduced their sensitive data footprint and proactively minimized the risks, costs and reputational damage of successful cyberattacks. Spirion provides greater command and control of sensitive data to leading firms across all industries from financial services to healthcare to public sector. Visit us at **spirion.com**

© 2020 SPIRION, LLC. ALL RIGHTS RESERVED