Privacy & Security Law Report®

September 11, 2017

Bloomberg BNA

Tax Practice

Consumer Law Requires Tax Preparers to Protect Against ID Theft

BNA Snapshot

- Gramm-Leach-Bliley Act applies to financial institutions—including tax businesses
- Weak Wi-Fi security biggest threat for tax professionals

By Kat Lucero

Tax professionals could be violating Federal Trade Commission rules if they aren't taking the proper steps to protect sensitive client data.

A nearly two-decade-old law designed to protect consumer data handled by banks and other financial institutions also applies to tax businesses. But not many tax return preparers know they should be paying attention to the Gramm-Leach-Bliley Act (Pub. L. No. 106–102), a 1999 law that requires companies to safeguard sensitive data and tell customers of their information-sharing practices, practitioners told Bloomberg BNA.

Last month, TaxSlayer LLC became the first tax preparation service to face charges of violating the law, an FTC spokeswoman told Bloomberg BNA. Hackers gained full access to nearly 9,000 accounts during two months in 2015 as a result of weak cybersecurity measures, an FTC complaint said. The Georgia-based private company settled with the commission on Aug. 29 and now has to enlist a third party to review its GLB compliance every two years for the next decade.

Cyberthieves can mine tax documents for Social Security numbers and other personal information to claim fraudulent individual and business tax refunds. The Internal Revenue Service said, for example, that it stopped nearly $11 billion in confirmed fraudulent refunds in 2015.

“If you get in, you get everything,” Larry Gray, a managing partner at AGC-Alfermann Gray & Company CPA's LLC of Rolla, Mo. said of the treasure trove of information collected by tax professionals, such as bank and investment accounts, Social Security numbers, medical records, and even business clients’ vendor data.

The IRS is receiving reports of “tax professional data breaches at the rate of three to five a week, a level that requires immediate attention,” the agency said in a Sept. 5 release as part of its 10-part-series campaign aimed at tax professionals called “Don't Take the Bait.” The latest release urged tax professionals to prioritize data security. In a July announcement the IRS said, “From January through May, there were 177 tax professionals or firms who reported data thefts involving client information involving thousands of people.”

FTC Enforcement

Financial institutions and tax professionals must comply with GLB's financial privacy and safeguard rules. The privacy rule requires companies to inform customers about their privacy policies and practices with an initial and annual notice, while the safeguard rule mandates that companies have measures to secure customer data.

TaxSlayer didn't follow either rule. It failed to provide a “clear and conspicuous initial privacy notice” and to “deliver the initial privacy notice so that each customer could reasonably be expected to receive the actual notice,” the FTC complaint said.

The complaint also said the company didn't have a written information security program, failed to conduct the necessary risk assessment, and failed to implement the safeguards to control those risks—specifically, the risk that hackers would use the

stolen credentials. As a result, hackers accessed nearly 9,000 users'accounts to commit identity theft, such as filing fake returns with altered routing numbers.

For years, most tax businesses flew under the radar of well-funded, tech-savvy criminals, who favored financial institutions, such as banks and creditors, as targets, according to Gray, who has been conducting data security training sessions around the country over the past year for the National Association of Tax Professionals.

Criminals shifted their focus to tax businesses when the financial services companies stepped up their cybersecurity measures, according to Gray, who is helping the FTC and the IRS lead a four-part cybersecurity webinar series for tax professionals.

'Lowest-Hanging Fruit'

Wi-Fi security is the most common threat for small businesses and tax practitioners, IRS special agents said in July at the first cybersecurity webinar.

Perpetrators "tend to go for the lowest-hanging fruit," Mark Kahler, IRS special agent in the Criminal Investigation unit and the national ID theft coordinator, said during the webinar.

Even if a tax professional doesn't use Wi-Fi for the work computer, there are machines that are connected to the wireless router, such as printers, tablets, and mobile phones. "That's how these guys work their way in," Kahler said.

Hackers are then able to obtain the tax professional's credentials "either through a phishing e-mail and/or link sent to individuals in the tax practitioner's office," Brian Thomas, an IRS special agent in the CI unit, said during the webinar.

Credentials such as electronic filing identification numbers, centralized authorization file numbers, and preparer tax identification numbers allow criminals access to various mainframes and client data, Thomas said.

Be Aware

Criminals are also familiar with various tax, accounting, and payroll software, so when they get into a computer network they know how to run the data, Thomas said.

Kahler said agents have seen advertisements on the online black market selling the tax businesses' assets, including the number of clients and the software used to store the accounts.

One ad, for example, described a business with 500 clients, each containing a dozen or more records, and the ability of the buyer to get full administrative rights with the software, Kahler said.

Delivering privacy policy notices by email or letter—the way consumers expect to receive them—is one tip the FTC gives for avoiding a case similar to the TaxSlayer one.

"A link to your privacy policy on your home page is insufficient," Lesley Fair, an attorney in the Consumer and Business Education Division, said in a blog post.

Fair also said GLB's safeguard rule doesn't build in any "laurel-resting time," so companies must evaluate and adjust information security programs whenever there are changes in business operations.

Tax professionals should also use appropriate authentication procedures and pick software that requires multi-factor authentication, such as a telephone call or text that gives legitimate users a personal identification number in addition to the login and password, Lisa Weintraub Schifferle, an attorney in the the same FTC division, said in another blog post.

"In this case, it was only after TaxSlayer Online started requiring multi-factor authentication that the hackers could no longer get into accounts," Weintraub Schifferle said.

To contact the reporter on this story: Kat Lucero in Washington at klucero@bna.com

To contact the editor responsible for this story: Meg Shreve at mshreve@bna.com