

A Privacy Check-Up Can Keep Advisors Out of Trouble

New state and foreign laws mean being ultra-careful about collecting and disclosing a client's personal data.

The ever-increasing confusing maze of *privacy* is critically important for advisors, my partner, Trina Glass, told me recently. She began by saying: "Perhaps, and I admit I am a bit biased, but the most important disclosure you are required to provide your client is your firm's Privacy Notice. Advisors are subject to the Gramm-Leach-Bliley-Act (GLBA), specifically Regulation S-P, which requires advisors to implement notice requirements and restricts the advisor's ability to disclose a consumer's nonpublic personal information (NPPI)."

The Privacy Notice must provide clients with notice of the firm's privacy policies and practices. If the advisor intends to disclose NPPI about a consumer to nonaffiliated third parties, the advisor must first provide certain corresponding disclosures to the client, giving them the ability to "opt-out" (i.e., prohibit the advisor from disclosing NPPI).

Does your privacy notice comply with Regulation S-P notice/disclosure requirements?

The last few years there has been the emergence of state and foreign privacy laws. Generally, if you are collecting or using personal information for purposes outside of providing financial products or services to your client *or* collecting NPPI not covered under the GLBA, then your firm may be subject to the evolving privacy obligations required by certain state and international privacy laws.

Moreover, some of these laws provide consumers with private rights of action. So annually when evaluating its compliance program, as part thereof, it is prudent for the advisor to conduct a Privacy



Check-Up to determine:

- Is your client deemed a consumer under the law? For example, certain individuals who interact with financial institutions may be considered "consumers" under the California Consumer Privacy Act (CCPA) but not under GLBA. Is your firm subject to the CCPA? Or any other state privacy law?

- What types of sensitive information and NPPI do you collect from your client? Is it covered under GLBA, if no, is it subject to other state privacy laws?

- How are you collecting sensitive information and NPPI from your client? Does your website use cookies? If yes, are you collecting sensitive information and NPPI that may not be covered under GLBA?

- Who and what has access to your client's sensitive information and NPPI and how does your firm monitor that access? For example, have you provided access to vendors or third parties outside the scope of your financial engagement?

- How do you use your client's NPPI? If used for any reason outside of the scope of providing financial services, have you advised and provided your client with a way to opt-out of that disclosure?

These are just a few of the preliminary questions that you will need to answer to determine whether your collection and use of your client's data is beyond the scope of the GLBA. Specifically, whether state and international privacy laws should be considered when evaluating and implementing a robust Privacy Program.

To address your firm's Privacy Readiness, first consider creating an inventory of the NPPI the firm collects:

- Determine all of the ways the firm collects NPPI. For example, client onboarding or website cookies;
- Determine where and/or how the NPPI is stored, i.e. in the firm's internal systems or hosted/stored by a third-party;
- Determine whether the initial and routine due diligence the firm conducts on third-party applications or vendors that collect, store and/or use your client's NPPI is sufficient;
- Determine how the firm protects client NPPI, including when employees access the NPPI from outside of the firm's offices or remotely; and
- Has the firm developed a comprehensive and reasonably adequate information security program around its collection, storage, access and monitoring of the client's NPPI?

If your client's data is breached, compromised or misused, the consequences could prove costly. Consider addressing your firm's privacy readiness with an experienced privacy attorney. **IA**

Thomas D. Giachetti is chairman of the Investment Management and Securities Practice Group of Stark & Stark. He can be reached at tgiachetti@stark-stark.com.