The use of participant data for provider marketing has become a hot topic—and a potential legal risk. By Judy Ward
“This whole participant-data privacy issue has legs,” says Fred Reish, a Los Angeles-based partner at law firm Faegre Drinker Biddle & Reath LLP. “There will be a lot more said about participants’ data privacy rights in the next 10 years.”

Several recent settlements of 401(k) plan lawsuits have addressed the use of participant data by recordkeepers. Reish anticipates more lawsuits dealing with use of participant data, and says plan fiduciaries need to get up to speed on how their recordkeeper and advisor utilize this data, and evaluate whether to limit that data’s use for marketing.

“The easiest fiduciary breach to prove is where a plan sponsor has done nothing about it,” Reish says. “Once you can show that a plan committee has investigated the issue and taken reasonable steps, it’s actually quite difficult to prove a fiduciary breach in this area. The key for fiduciaries is to be educated, and be thoughtful.”

A PLAN ASSET, OR NOT?
Is participant data a plan asset? And do plan sponsors have a fiduciary duty to limit marketing use of this sensitive data by providers? The law on that isn’t yet defined, Reish says.

ERISA doesn’t specifically discuss use of participant data, but several recent fee lawsuits that also allege misuse of participant data deals with this issue, Reish says. Each lawsuit focusses primarily on plan fees, but plaintiffs additionally alleged that the plan fiduciary didn’t do enough to protect participants’ data from the recordkeeper.

In Divane v. Northwestern University, the trial court found that the sponsor didn’t have a fiduciary duty to manage the use of participant data by its recordkeeper. The Divane appeal that the lawsuit got settled. “Because the lawsuits both say that the recordkeeper was overpaid, the settlements require the plan sponsor to engage in an RFP (request for proposal) process to get bids from recordkeepers,” Reish says. “These settlements also say that the new recordkeeping agreement has to prevent the recordkeeper from marketing additional investments and products beyond the plan to participants, unless they opt in to receiving that marketing. With this ‘opt-in’ approach, if a participant doesn’t opt in to the provider offering outside-the-plan services, products, and investments, the provider couldn’t promote them, and correspondingly, wouldn’t earn money from these products and services.”

St. Louis-based law firm Schlachter Bagard & Denton filed the Northwestern, Vanderbilt, and Johns Hopkins cases. In an interview, Senior Partner Jerry Schlachter talks about why he sees it as a breach if a plan fiduciary allows the use of participant data for marketing, without a participant’s consent.

“It starts with the fact that participant data is highly confidential,” Schlachter explains.
Recordkeepers have data such as a participant’s Social Security number, total account assets, and investment allocations. “This is the most confidential information you can have on someone, alongside health information, which is very protected,” he says. “And it’s not provided under anybody’s understanding that it will be used for other purposes, such as allowing the recordkeeper to try to sell participants additional services.”

Participant data is a plan asset because it is generated by the plan, Schlichter continues. “Why is it a violation of ERISA, even if it were not a plan asset? Because, while ERISA doesn’t speak specifically to participants’ data, it does speak to operating the plan in the exclusive best interests of participants,” he says. A provider using participant data to market additional products and services is operating in its own financial interests, and a plan fiduciary has a duty to understand that, he says. “The implicit backing of the employer also creates tremendous leverage for a service provider to stand alone in offering those products and services to participants,” he adds.

What should employers do about the use of participant data? Schlichter says explicitly prohibit the recordkeeper from using it for marketing without a participant’s consent, or leverage access to the participant data to negotiate better recordkeeping fees. “They should prohibit the use of that data,” Schlichter responds. “Would anyone contest that it would be highly improper for a doctor’s office to take the Social Security numbers and health information of its patients and sell it to pharmaceutical companies? No one would argue for that.”

To Thomas E. Clark Jr., chief operating officer and partner at Boston-based The Wagner Law Group, Schlichter’s legal thinking on use of participant data has several big holes. “The first hole is, whether participant data is a plan asset has not been mentioned in ERISA, or regulations put out by the DOL [U.S. Department of Labor],” Clark says. “Participant data is NOT provided under anybody’s understanding that it will be used for other purposes, such as allowing the recordkeeper to try to sell participants additional services.”

Four Keys to Working at Home Safely

You’re a valuable target for a cybercriminal, especially when you’re working remotely.

“If you’re a financial advisor, you’ve got a lot of information that’s of value,” says Baud Gué, partner and co-chair of the privacy and cybersecurity practice at law firm Fenner Spiegel LLP in Charlotte, North Carolina. “Sometimes, enough information could be accessible to steal money outright.”

To help protect participant data, keep the following in mind:

Access control only on a company device. Working at home this spring, Gué had two devices on his desk. “The company device is basically for all client work,” he says. “And the personal device, I use to access materials that are in the public domain.” Cybercriminals use technology to constantly scan for vulnerable devices, he says.

“If somebody is doing client work on their own device, at some point they are going to pick you up and flag you as a target,” he says. “And the reality is that a lot of the time, those places have been compromised. Somebody can be physically present in that same location, and intercept that data.”

Limit data access to employees who need it for their work. “Every network is only as strong as its weakest link,” Gué says. “A lot of our employees don’t need access to your sensitive material to do their job. Any aisle of information that is valuable, you want to lock down tight. If all your employees have access to data, somebody working remotely could have an unscrupulous brother-in-law, or an old computer that can easily be compromised.”

Keep doing cybersecurity practices drills. In addition to annual training, Gué says his law firm runs cybersecurity drills throughout the year. “We will send out mock messages constantly to our staff,” he says. “There are law firms that, if you click on a link in one of those emails, they will lock you out of the system, and then you have to go to a three-hour training and take an exam to get back into the system. We’ve introduced that draconian in our response. But the best way to prepare is to keep sending mock messages to your employees, and see how they react.”
Four Keys to Good Cyber-Liability Coverage

No matter how many precautionary steps an advisor takes to protect participants’ data, a cybercriminal may still find a way around them. So even careful plan advisors need good cyber-liability insurance coverage, says Tom Schraml, Philadelphia-based vice president, Lockton Affinity, the group program division of Lockton Companies, the nation’s largest privately held insurance broker.

Lockton Affinity, in partnership with the American Retirement Association, recently launched the Lockton Affinity Plan Advisors Insurance Program, which includes a cyber-liability policy specifically designed for retirement plan advisors. When looking for cybersecurity coverage, Schraml suggests paying special attention to these four keys:

Get coverage for fraudulent instruction requests. This protects an advisor in case a cybercriminal successfully submits a request for a fraudulent withdrawal from a participant’s retirement account, Schraml says. These incidents are happening already in cases where an adviser serves as plan fiduciary, he says, aided by fraudsters having gained access to the personal information of a participant (like a driver’s license number) they need to make the withdrawal request appear legitimate. But many policies don’t definitively state that they cover distributions stemming from fraudulent instructions, he says.

Have a policy that includes losses from participants’ accounts. Most of today’s policies only cover fraud if the advisor loses money, not if client funds are stolen, Schraml says. “Coverage for client funds is the missing piece of what an investment you need,” he says. “Just about every policy out there is written on a first-party basis, which means that it does not extend to a client account.”

Make sure there’s no “sub-limit” for fraudulent request coverage. Many policies have a sub-limit on coverage for certain types of incidents. “So even if you’ve got a $1 million policy, the coverage for a fraudulent-instruction request may only be $250,000, or it may be $50,000,” Schraml says. “Even the good policies that affirmatively state they cover a fraud instruction incident are generally pulling back on coverage for it, so they’re not exposing themselves to the whole policy dollar limit.”

Understand the policy’s internal-control requirements. “Be sure to know if your policy has any exclusions around the cybersecurity procedures you need to follow. A lot of cyber-insurance policies state that if you have this scenario happen and you didn’t have a process, or you didn’t follow it, then no coverage applies,” Schraml says. “I recommend formally establishing internal controls for withdrawal requests, making them public to everyone at your firm, and then enforcing the heck out of them.”

Two: There is no open market for participant data, so a recordkeeper may sell the data and profit from it.”

Third, the possibility that a recordkeeper may be able to make additional income itself from working with plan participants on other things is already built into the bidding process,” Clark continues. “If the recordkeeper believes it has the ability to earn additional fees from working with participants, it is going to lower the fees in its bid for a plan’s business. And the use of participant data is addressed in almost every major recordkeeping agreement I’ve ever reviewed. So from a legal perspective, even if it’s a plan asset, it’s already addressed in the service agreement.”

Chief Compliance Officer Phil Troyer of Overland Park, Kansas-based Resources Investment Advisors sees the potential problems with recordkeepers’ unfiltered use of participant data. “Do I think the issue needs to be addressed? Yes,” he says. “For a recordkeeper to slip in a language to the service agreement that essentially says, ‘You agree that we can mass-market all our products and services to your participants!’ is probably not a good idea.”

But Troyer has concerns that if use of participant data gets too restricted, it will prevent plan advisors from helping participants as much as they could. “We’re starting to get more pushback from clients who’ve read about the Vanderbilt case,” he says. “They’ve seen the publicity around the Vanderbilt case, and they now want to prohibit all access to the data for us. I explain to them that we have to coordinate things with the recordkeeper and custodian, and that requires us to have access to certain participant data. Also, there’s been a big push among employers for us to provide financial wellness education to their employees, and that means us being able to reach out to their employees about more than the retirement plan.”

There’s value in an advisory firm that knows a plan’s participants best giving them additional help with services like financial wellness education and rollover advice, Troyer believes. If participants can’t get that help from the plan advisor, he says, most would have to find for themselves. “Now the ‘wolves’ are going to try to get that money, and people have no idea what to do,” he says.

Three Main Options

Up to now, service agreements with recordkeepers haven’t directly addressed use of participant data, Rose says. “Virtually every recordkeeping agreement I’ve seen has a provision around the...
cybersecurity ground rules the recordkeeper agrees to follow,” he says. “But it is a good time to set up best practices,” he says. “They need to set up guidelines on who will have access to their employees. So, later on, they can say, ‘Yes, we understand how our participant data is being used, and we control who has access to it.’”

Plan fiduciaries have three main options to address the use of participant data for provider marketing, as Reish sees it. One is to tell the plan’s recordkeeper outright that it can’t use participant data at all to market non-plan products and services, and make that explicit in the service agreement. The second is to follow the approach used in the California Consumer Privacy Act, and require notification to participants on the use of their data, with the ability for them to opt out of their data’s marketing use. Or third, a plan fiduciary can allow marketing of non-plan products and services, and follow a sound process to ensure the fiduciary’s comfort that the additional products and services are helpful, reasonably priced, and of good quality,” he says.

Attorney Andrew S. Williams calls it “the first line of defense” against a potential lawsuit, for a plan fiduciary to impose restrictions in the service agreement on the provider’s ability to use participant information to market non-plan products and services. “[Plan] fiduciaries ought to give serious consideration to restricting the use of participant data, beyond the core use of data that is essential to plan administration,” says Williams, a partner at Galan Christie Taglia LLP in Chicago. “It’s not just a question of when the current contract expires; it’s a question that a fiduciary should be raising with the current provider and plan advisor, if they’re in the midst of a contract. And if I were an advisor, I’d proactively do a review with my clients, to do some clear lines around the permitted and non-permitted uses of plan data (by the advisor). Make sure that you’re on the same page as your clients on this issue, going forward.”

On the wealth management side of the business, Troyer says, Resources Investment Advisors is subject to the U.S. Securities and Exchange Commission (SEC) Regulation S-P, which covers privacy of consumers’ financial information. “It requires that an annual notice be sent to all our wealth management clients, explaining how we will use the information we have about them,” he says. The SEC has said that these regs don’t apply to retirement plans, only individuals. But for several years, we’ve treated our retirement plan clients as if Regulation S-P does apply to them.” So Resources voluntarily provides an annual privacy notice to its plan clients, which includes information regarding its use of the plan’s participant data.

Williams doesn’t anticipate an explosion of lawsuits centered on use of participant data. “I think that for the time being, it’s going to be an ancillary issue for these few lawsuits,” he says. “It seems like it’s not yet a juicy-enough issue for a suit that’s based just on the use of participant data. There’s a question of what the ‘dollars and cents’ would be for the plaintiff’s attorneys bringing the suit. Damages caused by non-plan use of participant data would be as difficult to establish as damages resulting from the rebo-back solicitations many of us receive every day.”

Asked about the potential for the spread of lawsuits alleging a fiduciary breach on use of participant data, Schlichter says he doesn’t think recordkeepers’ unrestricted use of participant data is unique to a few 401(k) plans. “I can say if this practice is the norm, but it is an increasing practice. From what we’ve seen, recordkeepers aren’t confining this practice to certain types of companies or businesses,” he says. “So plan fiduciaries should be on notice on this issue. There is a very simple rule that should be followed. When in doubt, fiduciaries should ask themselves the question, ‘Is this in the exclusive best interests of plan participants?’”