

Reproduced with permission from Tax Management Memorandum, 65 TMM, 07/31/2024. Copyright © 2024 by Bloomberg Industry Group, Inc. (800-372-1033) <http://www.bloombergindustry.com>

## Cut Cyber Breaches, Services Fees for Puerto Rico Benefit Plans

By Carlos Gonzalez  
BenefitsPuertoRico.com

*Puerto Rico benefits & compensation expert Carlos Gonzalez shares his practical experience with the evaluation of the cybersecurity measures of local financial institutions servicing retirement plans in operation in Puerto Rico.*

Sponsors of retirement plans operating in Puerto Rico, particularly in the wake of an Infosys security breach last November affecting entities throughout the world, have undertaken to evaluate the cybersecurity practices of local service providers that have access to sensitive information of plan participants. Pursuant to their fiduciary duties under the Employee Retirement Income Security Act of 1974, plan sponsors can and have negotiated to pay lower fees to those providers, such as Puerto Rico (“PR”) trustees, recordkeepers, and, to a lesser extent, paying agents.

The heightened attention to cybersecurity accords with U.S. Department of Labor / Employee Benefits Security Administration’s (EBSA) 2021 [guidance](#) including recommendations for a process retirement plan sponsors should follow to confirm that their service providers have in place strong data protection protocols,

Previously, even though the vast majority of these plans, be they PR-only qualified or dual-qualified plans, are subject to ERISA (see [ERISA §3\(10\)](#)), there was little action on the evaluation of the cybersecurity measures of local service providers. Apparently, plan sponsors were unaware that some of these providers have access to confidential information or assumed that the cybersecurity evaluation they performed in connection with their U.S. service providers also covered the local ones. As a result, most PR plans’ records did not include evidence that the cybersecurity measures of local service providers had been evaluated and found to be adequate, and the service agreements with those providers did not address cybersecurity matters.

Then the breach on Nov. 3, 2023 (see [Infosys’s statement](#)) brought to the attention of many companies the immediacy of cybersecurity threats to their retirement plans and deferred compensation arrangements. On review of their service agreements, they found that most did not include any terms or conditions regarding the local provider’s cybersecurity measures or contractual commitments in the event of a breach. This was particularly the case for agreements dating back to the 1990s and early 2000s and automatically renewing throughout the years. Moreover, the fees payable under some of the agreements, such as those for institutional trustee services, were higher than the current market rate for similar services. If, as is oftentimes the case, such fees were being paid out of plan assets, the companies had a fiduciary duty to negotiate lower fees.

### Which Providers Have Access to Confidential Information?

The first step in the cybersecurity evaluation process is identifying which of the local service providers have access to confidential information. The answer largely depends on whether the retirement plan is dual-qualified or PR-only qualified. Basically, a dual-qualified plan is a regular U.S. retirement plan that includes some PR employees among its active participants and is qualified under both [Section 401\(a\)](#) of the U.S. Internal Revenue Code of 1986, as amended (the “Code”), and [Section 1081.01\(a\)](#) (p. 418) of the PR Internal Revenue Code of 2011, as amended (the “PRIRC”); whereas a PR-only qualified plan is a plan established in Puerto Rico that only covers eligible PR employees and is qualified under PRIRC §1081.01(a), but not Code §401(a).

### Dual-Qualified Plans

When it comes to the PR aspects of cybersecurity evaluations, dual-qualified plans are the easiest because, except for a PR paying agent, all the service providers with access to confidential information are based in the United States. For example, the U.S. trustee that has legal title over the assets of U.S. participants also has legal title over the assets of PR participants, the same investment funds available to U.S. participants are available to PR

participants, and the U.S. recordkeeper that manages the accounts of U.S. participants also manages the accounts of PR participants. Therefore, the only cybersecurity measures that need to be evaluated are those of the U.S. service providers.

To help process the payment of benefits to their PR participants, however, some, but not all, dual-qualified plans use a local financial institution to serve as PR paying agent. PR participants request the payment from the U.S. recordkeeper, which transfers the corresponding funds and related payment instructions to the PR paying agent, which deposits the funds directly into participants' bank account or mails a check to their residence.

The PR paying agent is also responsible for complying with the local tax reporting and withholding requirements on distributions from qualified retirement plans, such as reporting the distribution to the PR Department of the Treasury (commonly known by its Spanish name as "Hacienda") by electronically filing local tax [Form 480.7C](#) through Hacienda's online portal, [SURI](#), and mailing a hardcopy thereof to the PR participant's residence. Form 480.7C requires various items of confidential information, such as the participant's name, address, and Social Security number. Therefore, to render its services, the PR paying agent needs access to that information.

If the U.S. recordkeeper is the one that engages the PR paying agent, the U.S. recordkeeper, not the plan sponsor, is responsible for evaluating the paying agent's cybersecurity measures. Accordingly, this obligation should be addressed in the recordkeeping services agreement between the U.S. recordkeeper and the plan sponsor, and the paying agent services agreement between the U.S. recordkeeper and the PR paying agent should specify the latter's cybersecurity-related obligations over confidential information.

On the other hand, a plan sponsor that directly engages the PR paying agent will assume responsibility for the evaluation and will be the signing counterparty in the paying agent services agreement.

### ***PR-Only Qualified Plans***

PR-only qualified plans sponsored by U.S. and international companies doing business on the Island are always funded through a PR-based trust fund established with a local financial institution, which serves as both PR trustee (i.e., it has legal title over plan assets) and PR paying agent (i.e., it completes all benefit payments to participants). At the very least, in its role as PR paying agent, the local financial institution will have access to confidential information, thus its cybersecurity measures need to be evaluated. Some PR-only qualified plans also

use a PR recordkeeper, but ordinarily this is the same local financial institution that serves a PR trustee and paying agent or an affiliate thereof (i.e., the local financial institution offers a bundled services arrangement). As such, only one cybersecurity evaluation process is needed.

In sum, for PR-only qualified plans the cybersecurity measures of the local financial institution that serves as PR trustee, paying agent, and/or recordkeeper should be evaluated. This is the case even for PR-only qualified plans that use a U.S. recordkeeper because, ordinarily, the local financial institution acting as PR trustee processes all benefit payments to PR participants. The plan sponsor, not the U.S. recordkeeper, is always the one that directly engages the local financial institution acting as PR trustee. Thus, the plan sponsor is responsible for this evaluation process.

### ***Other Local Service Providers***

What about accountants who audit the financial statements for the plan, attorneys who prepare plan amendments and get plans qualified with Hacienda, and third-party administrators who assist recordkeepers with employee communications and local nondiscrimination testing?

Ordinarily, these service providers do not have access to participants' confidential information because they do not need it for the rendering of their services. For example, local CPAs and attorneys can rely on general plan information and de-identified participant information for auditing plans and completing Hacienda filings, respectively. A best practice for minimizing cybersecurity issues on dealings with these non-financial local service providers is to de-identify as much as possible the individual participant information shared with them and encrypt all emails and files containing such information.

### **Cybersecurity Evaluation Process**

Before addressing the process that plan sponsors have generally followed for evaluating the cybersecurity measures of their local service providers, it should be noted that, in practice, most plan sponsors have limited leverage to force contractual terms and conditions on cybersecurity matters on their PR trustees and paying agents. Currently, only three local financial institutions — Banco Popular de Puerto Rico, BPAS Trust Company of Puerto Rico, Inc., and Oriental Bank & Trust — offer institutional trustee and/or paying agent services to retirement plans in Puerto Rico. Moreover, most of the retirement plans in operation on the Island are fairly small (i.e., fewer than 500 participants and less than \$50 million in assets), which

limits the fees local financial institutions generate for their retirement plan services.

As a result, local financial institutions have adopted a one-size-fits-all approach to cybersecurity compliance where customization or plan-specific changes are generally disallowed. Sponsors unwilling to accept the cybersecurity commitments and contractual provisions offered by their current PR trustee, paying agent, or recordkeeper may have no other option but to switch providers, and, even then, the new provider is bound to follow the same one-size-fits-all approach. Fortunately, pretty much all the plan sponsors that have evaluated the cybersecurity measures of their PR trustees, paying agents, and recordkeepers have found them to be adequate and consistent with EBSA guidelines.

Basically, the local cybersecurity due diligence process has progressed as follows:

1. The plan sponsor or its benefits advisor requests the service provider to provide copies of the service provider's cybersecurity compliance policy, business continuity and disaster recovery plan, independent auditor evaluation (e.g., an unqualified SOC 1 Type 2 audit report addressing the service provider's institutional trustee, paying agent, and/or recordkeeping operations), and cybersecurity liability insurance policies and declarations currently in effect.

2. After reviewing the service provider's documents, the IT officials of the plan sponsor participate in one or more videoconferences with the IT officials of the service provider to evaluate in further detail, among other things, the extent and nature of the confidential information used by the service provider, strength and effectiveness of its IT systems and infrastructure, history of data security incidents and incident responsiveness, security measures of data storage facilities, periodic risk assessments and independent auditor findings, level of cybersecurity liability insurance, employee training on cybersecurity matters, and procedures for management and disposal electronic information and computer equipment.

As noted above, by and large plan sponsors have concluded that the cybersecurity measures of local financial institutions are up to industry standards and no changes thereto are needed. And service providers have generally been willing to participate in as many conversations and provide as many documents as are necessary or appropriate to properly address the cybersecurity-related questions and concerns of their clients.

The contracts or agreements governing the service provider's services to the plan are then formally amended or restated to incorporate the service provider's cybersecurity duties and responsibilities. Contractual

provisions added to these agreements include the service provider's duties to follow its own cybersecurity compliance policy and EBSA guidelines on the subject, to update the policy and keep it in accordance with industry standards, to protect the privacy of the confidential information it receives and acknowledge the plan sponsor's ownership of such information, to perform periodic audits and risk assessments and provide a copy of the corresponding audit reports to the plan sponsor, to monitor and promptly notify any cybersecurity incident to the plan sponsor, to cooperate with proper resolution of cybersecurity incidents, and to keep adequate levels of insurance coverage.

If, as is usually the case for dual-qualified plans, the local financial institution only serves as PR paying agent, the new cybersecurity provisions should be incorporated into the corresponding paying agent services agreement. If the local financial institution also serves as PR trustee (as is the case with most PR-only qualified plans), the new cybersecurity provisions should be incorporated into the corresponding trust document. Pursuant to local law, PR trust agreements and amendments thereto must be prepared and executed through a notarized deed of trust, which is then registered with the local government (see Articles 5 and 7 of P.R. Act No. 219-2012, 32 L.P.R.A. [§3351d](#) and [§3352](#)). And if the local financial institution renders recordkeeping services to the plan, the corresponding recordkeeping services agreement should be amended accordingly.

### **Reduction of Fees**

Over the last five to 10 years, all the local financial institutions servicing retirement plans in Puerto Rico have lowered the fees they charge for institutional trustee and recordkeeping services (although not for paying agent services), driven by technology improvements and competitive pressures. It's part of a general reduction of fees and expenses of financial products and services, similar to U.S. mutual funds and brokerage firms lowering their fees. Insofar as it is also a positive byproduct of these cybersecurity evaluations, local financial institutions are not voluntarily lowering their fees absent a plan sponsor's request, and even when requested may try to hold the line and keep their fees as close as possible to the current fee schedule. But, in the author's experience, they will not risk losing a client over a reasonable fee reduction, especially if they know that their current fee is substantially above market rates. So any time a breach or an evaluation exposes a deficiency in a local service provider's cybersecurity practices, plan sponsors should use the occasion not only

## ARTICLES

to call for better compliance with established standards but also to formally request a renegotiation of fees.

*This article does not necessarily reflect the opinion of Bloomberg Industry Group, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.*

### **Author Information**

Carlos Gonzalez is President of BenefitsPuertoRico.com, a law firm assisting U.S. and international companies with Puerto Rico operations with employee benefits and executive compensation matters and is the author of Tax Management Portfolio 324-2nd T.M., *International Pension Planning – Puerto Rico*.