The Challenge of Protecting Personally Identifiable Information When U.S. Pension Plans Invest in U.K. and Luxembourg Private Funds

By: Edyta Brozyniak, Tobias Niehl, and Yuliya Oryol

It has never been as challenging for U.S. public pension plans and other institutional investors to clear KYC/AML/CTF requirements in certain foreign jurisdictions. Investors must figure out how to navigate the often-contradictory requirements of administrators, on behalf of counterparties and fund managers, who conduct background checks and identity verifications by requiring prospective limited partners in private funds to provide personally identifiable information (**PII**) as part of the due diligence process.

For U.S. public pension plans, negotiations over PII are often mired in prolonged negotiations intended to allay the investors' privacy concerns while simultaneously satisfying the necessary customer due diligence checks that the administrators are obligated to conduct before admitting the investors into the funds.

In general, PII is any data that could potentially be used to identify a particular person. Examples may include the person's full name, social security number, driver's license number, passport number, or bank account information. Private investors are generally more comfortable providing such PII information to open brokerage accounts to trade securities or invest in private funds. However, U.S. public pension plans and other institutional investors are limited by law, internal policies and/or established practices with respect to the types of information that they can publically disclose and, as a result, have pushed back on this requirement on behalf of their employees and trustees who are required to provide certain PII as signatories to fund documents. For U.S. public pension plans, negotiations over PII are often mired in prolonged negotiations intended to allay the investors' privacy concerns while simultaneously satisfying the necessary customer due diligence checks that the administrators are obligated to conduct before admitting the investors into the funds.

Given that many U.S. public pension plans seek to invest in the private funds managed by the European fund managers, we examine the underlying legislation in Luxembourg and the U.K. to ascertain what duties these jurisdictions impose on fund managers and their administrators and propose some solutions for consideration.

Luxembourg

The Luxembourg investment funds are obligated to identify their investors and beneficial owners (**BOs**).[1] Luxembourg fund managers and their administrators will therefore request PII from investors, their representatives and, if applicable, their BOs.

For individuals representing legal entities, administrators will at the minimum request the full name of the individual and a copy of such individual's ID card or passport.

The BOs of investment funds and the BOs of any company registered with the Luxembourg Register of Trade and Companies (*Registre de commerce et des sociétés* **RCS**) must be disclosed in the Luxembourg register of beneficial owners (*Registre des bénéficiaires effectifs* **RBE**).[2] If the pension plan investing in a Luxembourg fund would hold over 25% in commitments in that fund, its board of directors would be considered the BO of the Luxembourg fund and the names of such directors would be entered in the register.

If a fund is set up as a private limited company (*société à responsabilité limité* **S.À R.L.**), its shareholders must be disclosed in the RCS. If any S.À R.L. shareholders are individuals, the RCS must show any such individual's surname(s), forename(s) and date and place of birth.

The United Kingdom

The U.K. has had regulations intended to prevent money laundering in place for nearly 30 years. Such regulations have been influenced by the European Money Laundering Directives and the international standards set by the Financial Action Task Force (**FATF**).

Two main pieces of legislation address money laundering in England and Wales:

Back

The Challenge of Protecting Personally Identifiable Information When U.S. Pension Plans Invest in U.K. and Luxembourg Private Funds *(continued)*

1. Proceeds of Crime Act 2002; and
2. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (**MLRs**).

The MLRs set out criminal offenses for their breach.

"Relevant persons" (including fund managers) acting in the course of business in the U.K. must comply with these regulations, and are obligated to have appropriate systems and controls in place.

The MLRs allow a risk-based approach to AML, aiming to increase the efficiency and effectiveness of the systems and controls that fund managers put in place.

The JMLSG Guidance sets out what customer due diligence information must be provided by various types of customers.

JMLSG Guidance

Since 2006, the Joint Money Laundering Steering Group (**JMLSG**), a private sector body that comprises the leading UK Trade Associations in the financial services industry, has published guidance (**JMLSG Guidance**) *"to assist those in financial industry sectors represented on JMLSG by their trade member bodies, to comply with their obligations in terms of UK anti-money laundering* (**AML**) *and counter terrorist financing* (**CTF**) *legislation and the regulations prescribed pursuant to legislation."*

Because a private sector body publishes the JMLSG Guidance, it is not legally binding even though it has the approval of the HM Treasury. The most recent JMLSG Guidance was issued in June 2020 (and amended in July 2020). It provides *"a base from which management can develop tailored policies and procedures that are appropriate for their business."*

Risk-Driven Approach

The general approach taken when complying with the duties under the legal and regulatory framework relating to the AML and CTF legislation is risk driven. Therefore, money management firms should have in place policies and procedures that are appropriate and proportionate to the risks identified. It is important to note that the fund managers have some discretion as to how they apply the requirements of the U.K. AML/CTF regimes in certain circumstances with respect to their products, services, transactions, and customers.

Overseas Governments and Public Sector Bodies

The JMLSG Guidance sets out what customer due diligence information must be provided by various types of customers. For customers who are U.K. or overseas governments based in jurisdictions that the firm has determined to be low risk (or their representatives), supranational organizations, governmental departments, public sector bodies, state-owned companies or local authorities, the approach to identification and verification may be tailored to the circumstances of the customer, reflecting the fund manager's determination of the level of money laundering/tax fraud (**ML/TF**) risks presented.

In this context, it is important to distinguish between bodies engaged in public administration and state-owned bodies that conduct business. The nature of the business relationships established with the fund managers will therefore differ. Public administration involves a different revenue/payment stream from that of most businesses, and may be funded from government sources, or from some other form of public revenues.

State-owned businesses, on the other hand, may engage in a wide range of activities, some of which may involve higher risk factors, leading to a different level of customer due diligence being appropriate. Such entities may be partly publicly funded or may derive some or all of their revenues from trading activities.

Where the fund manager determines that the business relationship presents a low degree of risk of ML/TF, as

Back

The Challenge of Protecting Personally Identifiable Information When U.S. Pension Plans Invest in U.K. and Luxembourg Private Funds *(continued)*

may be the case with the U.S. public pension funds, standard due diligence measures may be applied. The JMLSG Guidance prescribes that the fund managers should obtain the following information about customers who are public sector bodies:

- full name of the entity
- nature and status of the entity
- address of the entity
- name of the home state authority
- names of directors (or equivalent)

The fund managers are also required to take appropriate steps to (i) understand the ownership of the customer, and the nature of its relationship with its home state authority; and (ii) be reasonably satisfied that the person the firm is dealing with is properly authorized by the customer and has authority to give instructions concerning the use or transfer of funds or assets.

Most U.S. public pension plans take the position that they are unable to provide PII in order to verify the identity of their signatories (either their employees or trustees) if the administrator requires government-issued identification for such individuals.

Signatories

For operational purposes, the fund manager is likely to have a list of those authorized to give instructions for the transfer of funds or assets, along with an appropriate instrument authorizing one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories must be verified on a risk-based approach.

Application

A study prepared by the U.K. Investment Management Association on the AML practices in the U.K. investment funds and investment management sectors in 2013 showed that most fund managers attempt to verify identities by alternative means before requesting documentary evidence from the customer. Such means comprise a combination of electronic checks and intermediary reliance.

For overseas public bodies/authorities, the fund managers uniformly require the signatory list. However, with respect to the verification of the signatories themselves, some fund managers apply a risk-based approach. Verification of an individual involves obtaining his/her full name, residential address, and date of birth.

Verification Requirements for U.S. Public Pension Plans

For those U.S. public pension plans investing in U.K. funds, the verification of the signatories is a cumbersome process. If the signatory's identity is to be verified from documents, such verification can be based on either a government-issued document which incorporates the individual's full name and photograph, and either his/her residential address or date of birth, or a government, court or local authority-issued document (without a photograph) which incorporates the person's full name.

In addition, there is a requirement for a second document—either a government-issued identification or a document issued by a judicial authority, a public sector body or authority, a regulated utility company, or another FCA-regulated firm in the U.K. financial services sector—which incorporates the customer's full name and his/her residential address or date of birth.

Alternative Approach to Verification for U.S. Public Pension Plans

Most U.S. public pension plans take the position that they are unable to provide PII in order to verify the identity of their signatories (either their employees or trustees) if the administrator requires government-issued identification for such individuals. For those U.S. public pension plans that have adopted these rules in written policy, there are real limitations on their negotiations with the fund managers or their administrators. In practice, if a compromise cannot be reached, such investors may be forced to forsake the investment.

Back

The Challenge of Protecting Personally Identifiable Information When U.S. Pension Plans Invest in U.K. and Luxembourg Private Funds *(continued)*

One alternative approach successfully utilized by many U.S. public pension plans is to provide an official employee identification badge in support of each individual's employment in lieu of copies of a driver's license, passport or utility bill. The individuals at issue here are employees of the governmental plan acting in their official capacities. As such, they are likely subject to the applicable state constitution where certain protections are afforded to employees of a public agency of that state. In fact, most state laws provide for a fundamental right to privacy, which should include the control of the disclosure of personal information. Furthermore, for the U.S. public pension plans that are subject to various public records and disclosure laws, PII may not be considered a public record and, therefore, may be exempt from the requirement of disclosure. In addition, most states treat an employee's home address, telephone numbers, and birth date within limited applicable exceptions to disclosure.

More established managers are often familiar with the verification process and may themselves suggest what supporting evidence can be provided in lieu of more traditional PII of individual government officials.

Furthermore, because the individuals in question are performing official duties in their capacities as public agency employees or trustees, they are unable to provide the requested government-issued identification or any other corroboration information, beyond submitting an official employee identification badge. In order to receive an employee identification badge, in most cases, the individual must be a current employee of the public pension plan or its sponsor and perform official duties in some official capacity. Prior to offering an individual employment, the governmental agency in question typically verifies all of the information provided by a prospective employee, which includes government-issued identification, and requires all prospective employees to submit fingerprints in order to conduct a criminal background check. In general, individuals whose identities cannot be verified or who fail a background check may not become employees of the plan. Although, of course, the employee or trustee may misrepresent his/her identity, the likelihood of this happening is extremely low particularly given that most state laws provide that it is a crime to provide false identification or otherwise misrepresent one's identity. In this regard, most of our clients have been able to successfully provide copies of work-issued badges without having to also provide administrators with additional identification, although we are aware that some administrators have also insisted during the negotiation process that the investor indemnify the manager in the event that it refuses to provide the required PII. Another approach is for the U.S. public pension plans to provide a "comfort letter" confirming the official capacities of the signatories. Such comfort letter may be issued internally by the plan's board or provided by an independent regulated entity (such as a bank). The type of documentation or information that is acceptable often varies from one manager to another.

We are aware of other creative methods by which managers and administrators have attempted to confirm the identities of the signatories, such as video conference calls where a manager or an administrator can confirm the identity of a signatory against his/her passport, but copies of the underlying documents are not provided to the manager or administrator.

Conclusion

Because the verification of signatories often proves to be a thorny issue when on-boarding U.S. public pension plans or other institutional investors, such verification is best approached at the onset of the fund review process so that the expectation of the parties with respect to what information is required to be provided by the investor, and what information is acceptable to the administrator, are addressed early on. More established managers are often familiar with the verification process and may themselves suggest what supporting evidence can be provided in lieu of more traditional PII of individual government officials.

Back

The Challenge of Protecting Personally Identifiable Information When U.S. Pension Plans Invest in U.K. and Luxembourg Private Funds *(continued)*

Finally, as more U.S. public pension plans continue to resist providing PII, managers and their administrators will likely become more comfortable over time with the U.S. approach to PII and find other creative ways to work around the KYC/AML/CTF requirements in order to accept U.S. public pension plans and other institutional investors into the European funds.

Edyta Brozyniak and Tobias Niehl *are Partners at Charles Russell Speechlys.* ***Yuliya Oryol*** *is a Partner at Nossaman.*

ENDNOTES:

[1]BO means any natural person who ultimately owns or controls the customer or any natural person for whom a transaction is executed or an activity is carried out.
[2]The following information on the beneficial owners of registered entities must be recorded and kept in the RBE:

1. name;
2. first name(s);
3. nationality (or nationalities);
4. the date of birth;
5. the month of birth;
6. the year of birth;
7. the place of birth;
8. the country of residence;
9. the precise private address or the precise professional address mentioning
   a. for addresses in the Grand Duchy of Luxembourg: the habitual residence listed in the national register of natural persons or, for business addresses, the locality, street and building number listed in the National Register of Localities and Streets, as provided for in Article 2(g) of the amended law of 25 July 2002 on the reorganisation of the administration of the land register and topography, as well as the postcode; and
   b. for addresses abroad: the locality, the street and the number of the building abroad, the postal code and the country;
10. for persons entered in the National Register of Natural Persons: the identification number provided for by the amended Act of 19 June 2013 on the identification of natural persons;
11. for non-resident persons not registered in the National Register of Natural Persons: a foreign identification number;
12. the nature of the effective interests held; and
13. the extent of the effective interests held.

Back