GLOBAL LEGAL INSIGHTS

Fund Finance 2026

10th Edition

Contributing Editor:
Wes Misson
Cadwalader, Wickersham & Taft LLP

FUND FINANCE association

glg Global Legal Group

TABLE OF CONTENTS

Jurisdiction Chapters

Data privacy and cybersecurity considerations for private fund sponsors during lender due diligence

Matthew D. Bivona
Corinne C. Musa
Natasha G. Kohne
Trevor L. Vega

Akin

Overview

In today's fund finance market, the intersection of data privacy, cybersecurity and lender due diligence has never been more critical. As private fund sponsors increasingly rely on subscription credit facilities, NAV facilities and other fund-level financings, the volume and sensitivity of investor data shared with lenders during underwriting continues to grow. Lenders routinely request access to, among other things, fund organisational documents, subscription agreements and investor side letters – often containing highly confidential information about institutional and individual investors.

This data exchange is essential for facilitating fund finance transactions, but it exposes sponsors to a complex web of legal, regulatory and operational risks. The evolving landscape of U.S. federal and state privacy laws, combined with heightened expectations for cybersecurity, means that sponsors must navigate not only compliance requirements but also reputational and commercial pressures from investors and lenders alike.

This chapter provides fund sponsors and their counsel with an overview of the current data privacy and cybersecurity landscape and explores some of the legal and practical implications for sponsors when retaining and sending investor data during the lender due diligence process. It also (i) highlights potentially applicable data privacy statutes and regulations under U.S. federal and state law, and (ii) discusses cybersecurity best practices, policies, and technical measures that sponsors can implement to improve the security of the lender due diligence process.

Relevant data privacy statutes and regulations under U.S. law

The United States has yet to adopt a comprehensive federal data privacy law. This puts the United States in sharp contrast to others, such as the European Union, which has adopted the General Data Protection Regulation.[1] However, the U.S. House Committee on Energy and Commerce has considered comprehensive data privacy legislation in each of the past three congressional terms, such as the American Privacy Rights Act and the American Data Privacy and Protection Act.[2] So, fund sponsors should be aware that the United States may enact a comprehensive federal data privacy law in the not-too-distant future and prepare

accordingly. In the meantime, funds (and their counsel) should consider the existing patchwork of U.S. data privacy statutes and regulations that are potentially relevant to retaining and transmitting investor data as part of the lender due diligence process, including the below.

Title V of the Gramm-Leach-Bliley Act ("GLBA")[3]

The GLBA is a federal statute that, *inter alia*, regulates the data privacy policies and practices of "financial institutions", a broadly defined term that includes entities whose business is engaging in certain financial activities, including "investing for others" and "providing … investment … advisory services".[4] Under the GLBA, certain federal agencies are empowered to impose privacy requirements on financial institutions.[5] The GLBA also provides its own requirements for handling "nonpublic personal information" ("NPI") of "consumers", which are commonly and collectively referred to as the "Privacy Rule". A "consumer" is an individual who obtains, from a financial institution, financial products or services that are to be used primarily for personal, family or household purposes (as well as such individual's legal representative).[6] NPI refers to nonpublic personally identifiable financial information provided by a consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer or otherwise obtained by a financial institution.[7]

Privacy Rule

At the time of establishing a customer relationship with a consumer,[8] and not less than annually during the continuation of such relationship if the financial institution's policies and practices have changed,[9] a financial institution must provide a clear and conspicuous disclosure to such consumer of such financial institution's policies and practices with respect to (i) disclosure of NPI to nonaffiliated third parties, including the categories of information that may be disclosed, (ii) disclosure of the NPI of persons who have ceased to be customers of the financial institution, and (iii) the protection of the NPI of consumers.[10] Both the initial and annual privacy notices must be made in accordance with the regulations promulgated by the relevant federal agencies given rulemaking authority under the GLBA.[11] These agencies have jointly developed a model privacy notice form, and if a financial institution uses such form in issuing its privacy notices, such financial institution will be deemed to be in compliance with the GLBA's disclosure requirements.[12]

Generally, financial institutions may not disclose NPI to a nonaffiliated third party unless such financial institution (i) provides or has provided the consumer with a compliant privacy notice, (ii) clearly and conspicuously discloses to the consumer that such information may be disclosed to such third party, (iii) gives the consumer an opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party, and (iv) gives the consumer an explanation of how the consumer can exercise that nondisclosure option.[13] However, these requirements do not prohibit the disclosure of NPI with the consent, or at the direction, of the consumer.[14] Where the GLBA's Privacy Rule applies, fund sponsors can avoid the administrative burden of complying with these requirements by securing investor consent to share NPI for the purpose of lender due diligence, either through the subscription documents or other written agreement.

The GLBA's privacy requirements extend beyond financial institutions themselves. Nonaffiliated third parties that receive NPI from a financial institution in compliance with the Privacy Rule cannot disclose such information to any other person that is not affiliated with the sending financial institution or the receiving nonaffiliated third party unless such disclosure would be lawful if made directly to such other person by the financial institution.[15] Where the GLBA's Privacy Rule applies, it is good practice for sponsors to notify lenders who receive investors' NPI of this obligation through a data protection provision in a written agreement with the lender.

Agency regulations under the GLBA

The GLBA provides various federal agencies with authority to impose privacy requirements on financial

institutions. Today, four agencies have GLBA regulations that may apply in the private funds context: (1) the Securities and Exchange Commission's ("SEC") Regulation S-P; (2) the Commodity Futures Trading Commission's ("CFTC") GLBA Rules; (3) the Consumer Financial Protection Bureau's ("CFPB") Regulation P; and (4) the Federal Trade Commission's ("FTC") Safeguards Rule.[16] These four separate sets of potentially applicable GLBA regulations are similar but not identical. As such, it is important for fund counsel to determine which entities in a fund structure may be covered by the respective regulations.

The content of these four regulations can be broken out into three categories: Privacy Rules; Safeguards Rules; and Disposal Rules. The Privacy Rules incorporate and build upon the GLBA's Privacy Rule (explained above), where the takeaway for sponsors is that consent from investors for disclosure to lenders is an essential component for any data sharing. Safeguards Rules, on the other hand, require covered entities to take certain steps to safeguard customer data. Finally, the Disposal Rules require covered entities to take certain steps to properly dispose of customer data. Once fund counsel has determined which entities in a fund structure are covered by the respective regulations, they should review what obligations, if any, each entity may have under the respective Privacy, Safeguards, and Disposal Rules, including before revealing NPI to a lender.

Agency	SEC	CFTC	CFPB	FTC
Regulation	Regulation S-P (17 C.F.R. § 248)	GLBA Rules (17 C.F.R. § 160)	Regulation P (12 C.F.R. § 1016)	Safeguards Rule (16 C.F.R. § 314)
Covered entities relevant to the private funds context	Investment advisers registered with the SEC.	Any of the following entities that are subject to the jurisdiction of the CFTC: • Futures commission merchants. • Retail foreign exchange dealers. • Commodity trading advisers. • Commodity pool operators. • Introducing brokers. • Major swap participants. • Swap dealers.	Entities in a fund structure that are "financial institutions" under the GLBA and are not otherwise covered by Regulation S-P or the CFTC's GLBA Rules. Thus, investment advisers that are not registered with the SEC would fall within the scope of coverage here.	
Privacy Rule?	Yes	Yes	Yes	No
Safeguards Rule?	Yes[17]	Yes	No	Yes
Disposal Rule?	Yes[18]	While the CFTC's GLBA Rules do not explicitly address disposal, the use of sufficient disposal policies and practices may be inferred from the Safeguards Rule at 17 C.F.R. § 160.30.	No	Yes

State privacy statutes

The potentially applicable laws and enforcement in state data privacy law are vast. To date, 19 states have passed comprehensive data privacy bills (i.e., bills intended to be comprehensive approaches to governing the use of personal information) and several other states are actively considering such legislation.[19] State

comprehensive data privacy bills typically provide some degree of exemptive relief for data or entities already regulated under the GLBA. Generally, these exemptions take two forms: (1) entity-level exemptions for financial institutions (as defined by the GLBA); and (2) data-level exemptions for NPI regulated by the GLBA. However, these exemptions are not uniform – some states exempt only the data, and others exempt the entity.

In the fund finance context, sponsors and their counsel must navigate a patchwork of state data privacy laws when sharing investor information with lenders. The complexity is heightened by multi-state investor pools and the multi-jurisdictional nature of private funds, which often have investors, entities, and operations in several states. Prior to sharing investor information with lenders, fund counsel should familiarise themselves with state data privacy laws (both comprehensive and non-comprehensive), particularly (i) in the states where entities within the fund structure are organised or do business and where investors reside, and (ii) in the states with strict privacy laws (e.g., California, Colorado, Texas) and with new or upcoming legislation. Below is a summary of the comprehensive privacy bills that have been passed to date as well as their GLBA-related exemptions.[20]

State	Legislation	Effective date	GLBA exemptions	
			Entity-level?	Data-level?
California	California Consumer Privacy Act; California Privacy Rights Act	January 1, 2020; January 1, 2023	No	Yes
Colorado	Colorado Privacy Act	July 1, 2023	Yes	Yes
Connecticut	Connecticut Data Privacy Act	July 1, 2023	Yes, but the exemption will no longer apply effective July 1, 2026	Yes
Delaware	Delaware Personal Data Privacy Act	January 1, 2025	Yes	Yes
Indiana	Indiana Consumer Data Protection Act	January 1, 2026	Yes	Yes
Iowa	Iowa Consumer Data Protection Act	January 1, 2025	Yes	Yes
Kentucky	Kentucky Consumer Data Protection Act	January 1, 2026	Yes	Yes
Maryland	Maryland Online Data Privacy Act	October 1, 2025	Yes	Yes
Minnesota	Minnesota Consumer Data Privacy Act	July 31, 2025	No	Yes
Montana	Montana Consumer Data Privacy Act	October 1, 2024	No	Yes
Nebraska	Nebraska Data Privacy Act	January 1, 2025	Yes	Yes
New Hampshire	Senate Bill 255	January 1, 2025	Yes	Yes
New Jersey	Senate Bill 332	January 15, 2025	Yes	Yes

State	Legislation	Effective date	GLBA exemptions	
			Entity-level?	Data-level?
Oregon	Oregon Consumer Privacy Act	July 1, 2024	No	Yes
Rhode Island	Rhode Island Data Transparency and Privacy Protection Act	January 1, 2026	Yes	Yes
Tennessee	Tennessee Information Protection Act	July 1, 2025	Yes	Yes
Texas	Texas Data Privacy and Security Act	July 1, 2024	Yes	Yes
Utah	Utah Consumer Privacy Act	December 31, 2023	Yes	Yes
Virginia	Virginia Consumer Data Protection Act	January 1, 2023	Yes	Yes

These state data privacy laws may govern things like a sponsor's obligations with respect to future use of data and any notices required in the case of a particular data breach. These laws also can speak to an investor's rights with respect to particular information that they have shared, ranging from whether an investor can force deletion of such data or corrections of such data. Non-compliance with applicable privacy laws can result in investigations, fines and enforcement actions by regulators.

FTC Act

Under the FTC Act, the FTC can enforce against unfair or deceptive acts or practices in or affecting commerce.[21] Pursuant to this authority, the FTC has pursued legal action where entities have made misleading claims regarding consumer data privacy and/or failed to take sufficient steps to safeguard customer data. Recent examples include an allegation that Facebook violated its privacy promises to consumers and finalisation of an order requiring Marriott and Starwood Hotels to settle charges that they failed to implement reasonable data security, leading to data breaches.[22] These cases highlight the need for fund sponsors to be transparent about data privacy policies and invest in cybersecurity best practices, policies, and technical measures.

Cybersecurity best practices, policies, and technical measures

Fund sponsors face a growing body of potentially applicable U.S. data privacy law and, depending on the context, may also have to comply with extensive non-U.S. legal requirements. However, sponsors may not only face *legal* liability stemming from their data privacy policies and practices – the financial and reputational harm associated with a cybersecurity incident can be significant, especially in the lender due diligence context, where sensitive data of high-net-worth individuals may be at stake. Investors (especially institutional ones) are highly sensitive to how their data is handled. Mishandling data or failing to honour privacy rights can damage a fund sponsor's reputation, harm investor relationships and make future fundraising more difficult. Further, what constitutes "adequate data protection" is everchanging due to new and amended data privacy and cybersecurity laws. As a result, meeting this standard will require consistent and adaptable monitoring, training and management buy-in.

Given the legal, reputational and financial risks at stake, how are sponsors practically supposed to comply with diligence requests from lenders that include sensitive investor information? It is rare, though not unheard of, for a borrower to require that lenders conduct due diligence in-person in a windowless

conference room, but the reality is that most fund borrowers transmit this confidential data to potential lenders through some electronic means. In doing so, fund borrowers should consider (i) whether the information they need to send includes the sensitive investor data of high-net-worth investors (including, e.g., social security numbers ("SSNs"), driver's licences or passports, or similar identifying information), (ii) where and how they plan to send the information, and (iii) what data privacy and cybersecurity requirements might apply based on the relevant laws, regulations, and policies of the fund. Before sending sensitive investor information to lenders, sponsors should consider adopting best practices, policies, and technical measures, including the below.

No email

When a fund sponsor has sensitive investor data to transmit, sending such information over email is never recommended. Emails can be hacked, devices lost, and login information exposed. Instead, sponsors should look for secure methods like dedicated enterprise file sharing platforms designed for secure transfer of documents and information. Reputable software-as-a-service ("SaaS") providers will offer enterprise-grade security to protect data on the system.

Use permission controls

Fund sponsors should make use of file sharing platform features that enable user permissions to be set and attach expiry dates to shared files that revoke access after a specified period. This will enable restricted access to files and prevent the files from being saved or printed, helping safeguard against data exposure. Sponsors should also monitor and control who is sending the information and ensure these persons are sending only the specific information being requested (i.e., avoid sending additional, unnecessary sensitive information).

Use appropriate data safeguards

Many data privacy and security laws mandate appropriate administrative, technical, and physical safeguards. These can include, among other measures, encryption of data at rest and data in transit, strong passwords, firewalls, and multi-factor authentication ("MFA"). Fund sponsors must ensure their safeguards are compliant with all relevant laws. In addition, based on the demands of the market as well as the fund's budget and risk tolerance, sponsors should decide whether safeguards over and above any legal mandates should be implemented. After implementation, these safeguards should be incorporated into employee training.

Implement cybersecurity training for employees

One survey showed that 66% of chief information security officers identified human error as their top cybersecurity risk, with 92% reporting data loss from departing employees.[23] This statistic highlights the importance of robust cybersecurity training for employees in order to mitigate the risks of a cybersecurity incident. All employees should partake in interactive training programmes that cover the cybersecurity risks that they may face in their day-to-day work, including malware, social engineering, phishing emails, using public WiFi networks, and double-checking email senders and links.[24] The nature of cybersecurity risks is constantly evolving, and employee training should be periodically updated to address new threats and modern developments.[25]

The lender due diligence process provides a unique opportunity for bad actors to gain access to sensitive investor data through human error. For example, in the flurry of receiving and responding to due diligence requests from the lender, a bad actor using a dupe email address may ask an employee to send a one-off email with an investor's SSN to avoid the hassle of uploading it to the data room. Employees that support the lender due diligence process should be provided with specific cybersecurity guidance above and beyond the all-employee training.

Manage service providers and supply chain risks

Fund sponsors increasingly rely on a diverse array of third-party service providers, such as file management platforms, cloud storage vendors, IT consultants, and data room operators, to facilitate fund operations and lender due diligence. While these partnerships can enhance efficiency and scalability, they also introduce cybersecurity risks that may arise from vulnerabilities in the supply chain. Sponsors should conduct thorough due diligence before onboarding service providers that will access, process and store confidential fund or investor information, including reviewing any security certifications (such as SOC 2 Type II, ISO/IEC 27001), incident response capabilities, data protection policies, and history of security incidents. Contractual agreements with service providers can cover technical, administrative and physical safeguards for information, as well as notification and cooperation during security incidents. Cybersecurity risk management does not end at the onboarding stage, so sponsors should periodically review service provider compliance with contractual obligations, monitor for changes in ownership or control, and stay informed about emerging threats affecting the provider's sector.

Include data protection provisions in written agreements with the lender

Fund sponsors do not want their investors' data to be at risk after handing it off. Written agreements with a lender receiving investor data should set forth such lender's obligations regarding that data. These written agreements may include a signed term sheet or engagement letter with enforceable confidentiality provisions or an executed credit agreement. Agreements should establish (i) how the data will be transmitted, (ii) how the recipient will store it, (iii) how long they will retain it, (iv) what purpose it will be used for, and (v) how it will be safely returned or deleted when that purpose is complete. Sponsors should ensure that the recipient will not (i) further transfer the information insecurely with a method not otherwise approved, (ii) transfer the information to other unintended parties, (iii) retain the information indefinitely, nor (iv) use it for some purpose other than what was specified.

Plan and practise for when something goes wrong

If all else fails and sensitive investor data is leaked, fund sponsors must be prepared. Sponsors should engage an interdisciplinary team, including legal, IT, finance, and management, to establish and periodically update an Incident Response Plan ("IRP").[26] The IRP should clarify the roles and responsibilities for responding to a cybersecurity incident and provide guidance on the key tasks that must be completed once the incident is identified.[27] It should also identify a list of key people who are tasked with responding to a cybersecurity incident.[28] Then, using the IRP, the response team should practise responding to a cybersecurity incident. Simulated exercises are a good way to practise responding quickly and effectively when a cybersecurity incident occurs. Simulations can include assessments of insurance carrier notification timelines, as well as decision-making on the timing and content of notifications to regulators.

Conclusion

The areas of data privacy and cybersecurity continue to develop at a rapid pace. Complying with the evolving legal landscape requires the close attention of fund sponsors, as lawmakers continue to implement new legislation intended to protect consumer data. More than ever before, it is critical that sponsors engage counsel that has a firm grip on the applicable legal requirements. This is especially true in the lender due diligence context, where a misstep in retaining or sending sensitive investor information may draw the attention of state and/or federal regulators. Similarly, the heightened financial and reputational risks associated with transmitting sensitive investor data to lenders call for adherence to cybersecurity best practices, policies, and technical measures. Of course, no amount of preparation can render a sponsor invulnerable to increasingly sophisticated bad actors. However, proper preparation can assist greatly in preventing a breach and in mitigating the adverse effects on fund sponsors, on investors and on lenders.

Acknowledgments

The authors would like to thank Joseph Hold and Calvin Robinson for their valuable contributions to this chapter.

Endnotes

1 https://gdpr-info.eu

2 https://iapp.org/news/a/congressional-committee-kickstarts-new-federal-privacy-law-dialogue

3 15 U.S.C. § 6801.

4 15 U.S.C. § 6801; 15 U.S.C. § 6809(3)(A); 12 U.S.C. § 1843(k).

5 15 U.S.C. § 6801(b); 15 U.S.C. § 6803(e); 15 U.S.C. § 6804.

6 15 U.S.C. § 6809(9).

7 15 U.S.C. § 6809(4)(A).

8 When a customer relationship is technically "established" for purposes of the rules, it is governed by the regulations promulgated by the federal agencies given rulemaking authority under the GLBA. 15 U.S.C. § 6809(11).

9 15 U.S.C. § 6803(f).

10 15 U.S.C. 6803(a); for additional details on the GLBA's notice content requirements, *see* 15 U.S.C. § 6803(c). "Nonaffiliated third party" is defined as any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution. 15 U.S.C. § 6809(5).

11 15 U.S.C. § 6803(b).

12 15 U.S.C. § 6803(e)(4).

13 15 U.S.C. § 6802(a)–(b).

14 15 U.S.C. § 6802(e)(2).

15 15 U.S.C. § 6802(c).

16 Updates to the FTC's Safeguards Rule took effect in May 2024, requiring certain financial institutions to adopt specific requirements related to reporting on data breaches and security events, such as notifying the FTC as soon as possible but no later than 30 days after discovery of a breach involving the information of at least 500 consumers.

17 Note also that 2024 amendments to Investment Advisers Act Rule 204-2 require investment advisers registered with the SEC to retain, *inter alia*, the following written records: incident response policies and procedures; documentation of any detected unauthorised access to or use of certain customer data, as well as any response to, and recovery from, such unauthorised access to or use of such data; and documentation of any investigation and determination on whether notification is required, notice transmitted, or U.S. Attorney General communications delayed. Also in 2024, the SEC adopted amendments to Regulation S-P, expanding the scope of information covered by the SEC's Safeguards Rule, and including certain data breach notification, incident response programme and recordkeeping requirements. The new requirements of Rule 204-2, as well as the SEC's Safeguards Rule, went into effect on August 2, 2024. The compliance date for the new requirements of Rule 204-2 and the SEC's Safeguards Rule is December 3, 2025 for "larger entities" (i.e., registered investment advisers ("RIAs") with $1.5 billion or more in assets under management ("AUM")). "Smaller entities" have a compliance date of June 3, 2026.

18 The SEC's Disposal Rule went into effect on August 2, 2024. The compliance date for "larger entities" (RIAs with $1.5 billion or more in AUM) is December 3, 2025. The compliance date for "smaller entities" is June 3, 2026.

19 https://iapp.org/resources/article/us-state-privacy-legislation-tracker

20 For a more detailed summary of state comprehensive data privacy bills, *see* https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

21 15 U.S.C. § 45(a)(1).

22 https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter; https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3022-marriott-international-inc-starwood-hotels-resorts-worldwide-llc-matter

23 https://www.proofpoint.com/us/newsroom/press-releases/proofpoint-2025-voice-ciso-report

24 https://www.contrastsecurity.com/security-influencers/6-cybersecurity-best-practices-to-secure-sensitive-data-contrast-security

25 https://www.contrastsecurity.com/security-influencers/6-cybersecurity-best-practices-to-secure-sensitive-data-contrast-security

26 https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

27 https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

28 https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Matthew D. Bivona

Tel: +1 214 969 2702 / Email: mbivona@akingump.com

Matthew's practice includes all aspects of finance, corporate and securities law. He represents borrowers and lenders in secured and unsecured credit facilities and other lending arrangements, issuers in connection with issuances of high-yield debt securities in Rule 144A and Regulation S offerings, private placements and restructuring transactions, and debtors and creditors in distressed debt restructurings.

Matthew advises both borrowers and lenders on a wide range of fund finance transactions, including subscription facilities, NAV facilities and management fee and GP facilities. He also advises clients in the real estate and hospitality industries in a wide range of financing activities, including mortgage and mezzanine lending arrangements, private equity and joint ventures.

Corinne C. Musa

Tel: +1 212 872 1045 / Email: cmusa@akingump.com

Corinne's practice focuses on borrowers and alternative lenders in all aspects of fund financing transactions, with a specific focus on subscription credit facilities, NAV and hybrid credit facilities. She also regularly represents clients on management fee and GP lines of credit and other financings throughout an investment fund's structure.

Corinne has been lead counsel on many of the largest and most complex credit arrangements to funds affiliated with preeminent fund sponsors. She partners with clients to provide meaningful and practical advice across the spectrum of fund financing transactions. Additionally, Corinne has experience advising on more general corporate finance transactions, including acquisition financings, and complex domestic and cross-border transactions.

Natasha G. Kohne

Tel: +1 415 765 9505 / Email: nkohne@akingump.com

Natasha is a recognised leader in complex U.S. and cross-border investigations and litigation involving financial institutions, sovereign entities, investment funds and technology companies.

With over two decades of experience, Natasha has become a trusted advisor to boards of directors and sovereign entities. She navigates complex dynamics involving foreign investment, national security, crisis management, and corporate governance. Natasha advises global entities at the intersection of national security and foreign investment, particularly in areas that intersect with technological advancement such as AI, cybersecurity, and data protection.

Trevor L. Vega

Tel: +1 214 969 4208 / Email: tvega@akingump.com

Trevor advises public and private clients on a wide array of corporate matters, including finance transactions, mergers & acquisitions and securities offerings.

Akin

One Bryant Park, New York, NY 10036, USA

Tel: +1 212 872 1000 / URL: www.akingump.com

Global Legal Insights – Fund Finance provides in-depth analysis, insight and intelligence across one industry viewpoint, 31 expert analysis chapters and 19 jurisdictions, covering key industry trends and developments including:

- Fund formation and finance
- Net asset value facilities
- Hybrid facilities
- Subscription lines
- Enforcement
- Secondaries
- Ratings
- Collateralised fund obligations

Written by leading industry participants from across the industry, this is the definitive legal guide for the global fund finance industry in 2026.

globallegalinsights.com