EisnerAmper

www.eisneramper.com

Q3 2016

Asset Management Intelligence

A publication from The Financial Services Group

Opportunities and Challenges for U.S. Managers Accessing Capital in Europe: Why Europe?

By Ray Kelly

As a source of investment capital, Europe is a key market for hedge funds. It is estimated that total assets under management ("AUM") in Europe increased by approximately 15% in 2014 to reach an all-time high of €19 trillion, while total assets of the continent's asset management industry grew 74% between end 2008 and end 2014.[1]

In light of the evolving European regulatory environment since the financial crisis, the supply-demand characteristics of the distribution landscape have shifted dramatically, and the result has been a dearth of high-quality U.S.-located products for EU investors. European investors are sophisticated and given current circumstances, are keen on exploring new opportunities. For those U.S. managers with viable strategies, opportunity knocks.

ROUTES TO MARKET

Interested parties have a number of different routes to market, from fully registered approaches [either Undertakings for Collective Investment in Transferable Securities ("UCITS") or Alternative Investment Fund ("AIF")] to national private placement regimes ("NPPR") and reverse solicitation.

The UCITS directive, for instance, provides managers with a "passport" to market open-ended funds to retail customers throughout the EU. Though mainly limited to traditional approaches, funds that employ strategies such as long-short or qualifying collective investment schemes that meet UCITS guidelines regarding diversification, leverage and risk management may still be eligible.

For non-traditional firms, there's the AIF option, which, under the Alternative Investment Fund Managers Directive ("AIFMD"), requires that alternative managers in Europe maintain robust operational transparency on behalf of investors and regulators. This includes frequent and detailed reporting on investment practices, executive-compensation disclosures, and other critical data. As the application of AIFMD can differ from one EU country to the next, firms that operate in multiple jurisdictions will need to be aware of specific rules within each of the participating member countries.

DEVELOPING A SUCCESSFUL DISTRIBUTION STRATEGY

So what is the most appropriate route to properly access this thriving marketplace? The simple answer is there is no simple answer, as the rules vary depending on whether an investment manager has a UCITS registered for local sale, a non-locally registered UCITS, a European AIF or a non-European Economic Areas ("EEA") AIF.

Option one involves registering as a UCITS established in the EEA (consisting of the EU plus Norway, Iceland, Switzerland and Liechtenstein) and the fund is then freely available to any EEA investor when registered locally. A UCITS offers a number of attractive marketing opportunities, including the ability to distribute across additional markets such as Hong Kong, Singapore, Taiwan, Chile and other regions. There are some notable challenges with these vehicles, however, including restrictions on certain types of investment strategies, as well as the need to offer investors daily (or at least bi-weekly) liquidity.

If the UCITS restrictions cannot be achieved, then generally speaking most European AIFs are passport-eligible (exceptions being investment managers with AUM under €100m or where a fund has 85% plus of its assets invested in one or more non-EEA funds).

In addition, AIFs can often utilize non-principal private residences ("NPPR") exemptions. Subject to the NPPRs in place in each EU member state, private placement may be available to U.S. Managers marketing AIFs, whether EU or non-EU AIFs.

U.S. managers may be able to continue to make use of NPPRs until at least 2018, subject to a number of mandatory conditions which will apply over and above the private placement rules operating from jurisdiction to jurisdiction. Unless and until the AIFMD passport is extended to third countries including the US, NPPRs will be the sole regime available to non-EU AIFs and non-EU managers wishing to market in the EU.

U.S. managers may be able to continue to make use of NPPRs until at least 2018, subject to a number of mandatory conditions which will apply over and above the private placement rules operating from jurisdiction to jurisdiction.'

Under certain circumstances reverse solicitation — a.k.a. "passive marketing" (i.e., where the investor contacts the manager) — may also be used as a gateway to the EU; however, it is a method of last resort and therefore should not be viewed in the same light as deliberate use of a passport or private placement exception. A non-solicited approach does not involve marketing — that is, investors access the fund manager, rather than the other way around. Managers that go this route should have air-tight compliance measures along with a clear and verifiable paper trail.

THE RIGHT ROUTE

Choosing between UCITS or AIF often depends on a fund's liquidity characteristics, as well as the type of investor the fund wishes to target.

When funds are entering a 'friendly' jurisdiction such as the UK, for instance, using private placement is a relatively straightforward process and may suffice at least during the initial marketing phase. Almost half of European hedge fund investors reside in the UK, which is yet another positive for foreign interests since from a regulatory perspective the UK is by far the most accessible territory within the region. Obviously any distribution strategy targeting the UK will need to consider the implications of the country's recent vote to leave the EU – the implications of 'Brexit' are currently unclear and are likely to remain so in the short-term.

While a little more complex than the UK, Switzerland is also an attractive target with a relatively straightforward and inexpensive approval process.

As additional jurisdictions are targeted, however, it may become more efficient for managers to fully register the fund. For example certain countries (Germany, France, Italy and Spain included) have only a limited appetite for funds outside the UCITS format.

While there are certainly challenges in accessing European investors, for those U.S. managers with the right product it may be a challenge worth consideration given the size of the market opportunity. ■

[1] *Asset Management in Europe, 8th Annual Review, European Fund and Asset Management Association, April 2015*

Ray Kelly is a partner with EisnerAmper Dublin. For more information, feel free to contact him at +353.1.293.3449 or ray.kelly@eisneramper.ie.

Vendor Management of Investor Data

By Maarten Robberts, Partner, Atlas Fund Services

As the U.S. moves closer to the internationally accepted Anti-Money Laundering ("AML") and Know Your Client ("KYC") standards, investors are left with the questions about what happens to their personal confidential information.

Historically, non-bank-affiliated financial institutions, such as administrators, have not been subject to specific AML regulations. Instead, most non-financial institutions in the United States have relied on best practices. Foreign countries often have more stringent requirements than the United States.

However, the U.S. regulatory environment is changing at a rapid pace. The new Financial Crimes Enforcement Network ("FinCEN") proposed regulations attest to this change. The recently proposed rulings by FinCEN further require financial firms to identify Ultimate Beneficial Owners ("UBOs"), to create risk profiles and to track business activities. Investor identification and UBOs have been subject to changing global and local reporting standards for decades.

Past attempts by non-bank-affiliated financial institutions to enforce revised AML and KYC compliance policies and procedures were often met with client resistance. Recently, however, clients such as fund investors, for example, have become increasingly concerned about the safety and safekeeping of their personal and confidential data.

Non-bank affiliated financial firms are required to ensure their current procedures for acquiring, validating and storing client information from custodial accounts meet market standards. In addition, the firms must update the information where necessary and comply with revised regulations that are more aligned with internationally accepted standards. The key challenges of the newly proposed AML-KYC rules and regulations are the implementation of technology, the expansion of account opening procedures, the authentication of existing client data, and client education. The process of ongoing digitalization of records and rapidly improving technology is both an asset and potential liability where there is an ineffective internal cybersecurity program and/or a weak governance framework to manage cybersecurity risks.

In 2015 and 2016, the SEC's Office of Compliance Inspections and Examinations ("OCIE") underscored the importance of vendor management, risk assessment processes and cybersecurity as their top priority. The industry now needs to be prepared for its attention to cybersecurity, compliance and controls during regular OCIE examinations. Investor identification, verification and data protection for the beneficial owner accounts held at broker-dealers and investment advisors are targeted specifically. Although non-bank-affiliated institutions may not be subject to these examinations, these firms will be held to the same standards.

COLLECTION, VERIFICATION AND SAFE-KEEPING

The purpose of the AML and KYC collection processes is to confirm assets are received from legitimate sources, prevent money laundering and deter terrorist financing. Service providers/vendors responsible for collecting client information must ensure qualified staff is assigned to handle and secure client data, and that the procedures and systems in place are tailored to provide for ongoing client data monitoring. The client (ultimate beneficial owner or "UBO") identification procedures must drill down to the level of a natural person or persons, and verification of the information validity and consistency should be checked against the lists issued by U.S. Office of Foreign Asset Control ("OFAC") and databases such as WorldCheck and WorldCompliance for criminal records and politically exposed persons.

In 2015 and 2016, the SEC's Office of Compliance Inspections and Examinations ("OCIE") underscored the importance of vendor management, risk assessment processes and cybersecurity as their top priority. The industry now needs to be prepared for its attention to cybersecurity, compliance and controls during regular OCIE examinations.

Storage of all printed and digital information should be subject to restricted access for authorized and supervisory personnel only. Printed materials containing personal tax information and social security numbers should be illegible/blocked prior to saving/storing the files. The files should be encrypted when stored digitally. After working hours, confidential client information should be securely stored and locked. With senior management oversight and approval, different levels of access can be established to safeguard investor profiles and activity. With respect to client/investor information, whether electronic or in physical form, access should be limited to a minimal number of users on a "need to know" basis.

Encryption of sensitive data adds an additional layer of security. Though it's not foolproof, it presents added hurdles in case of a security breach. With the various encryption technologies available in today's market, data encryption can present potential operational challenges such as the restoration of encrypted backed-up files when dealing with outdated encryption software. Organizations will need to evaluate all possible consequences of encryption and consider the long holding periods required to retain client records.

In light of the current compliance environment, the various layers of security and proper risk governance allow for peace of mind and mutual benefits to all parties involved. With or without an enforced regulatory framework, safeguarding of sensitive information has become a priority to the financial services industry. ■

Maarten Robberts is a partner at Atlas Fund Services, a global fund administration solutions provider. Questions? You can contact Maarten at +(5999) 845 3230 or mrobberts@atlasfundservices.com.

Navigating Operational Due Diligence in Emerging Markets

By Claudia Osmar

Emerging markets, such as those in Latin America, can be highly profitable. The costs are low and the markets are eager to attract foreign investment. However, they also involve certain risks, ranging from potential political problems to simple differences in business culture.

In developed markets, investors often limit the scope of operational due diligence to traditional financial and tax issues. This approach may fall short to uncover important information in an emerging market.

In emerging markets, the most difficult areas to navigate generally relate to the political environment, lack of transparency, bureaucracy and corruption. The traditional approach to operational due diligence is not enough to respond to the unique and specific challenges that exist. Sophisticated investors utilize a more integrated due diligence approach focusing on areas beyond traditional financial information.

KEY FACTORS TO CONSIDER DURING EMERGING MARKETS OPERATIONAL DUE DILIGENCE

A local team is crucial	In places where the line between businesses and government interests is sometimes blurry, understanding the culture of the emerging market and establishing a presence in the local market is a fundamental part of the process. Local teams are a key factor to success as they will have relationships and connections that enable them to understand and navigate the country's regulatory environment.
Reputational concerns	Higher importance should be placed on the reputation of the local company and its management. Getting to know the people is as relevant as a good track record and reputational due diligence should be part of the process.
Lack of transparency	One of the most important reasons for investors breaking off deals is a lack of transparency. In emerging markets, many businesses are family owned and companies might have a poor track record or lack of audited information. Often the quality of information is questionable (accessibility and accuracy) and it must be supplemented with on-the-ground work and interviews. It is not unusual to find multiple sets of books. Investors might engage auditors and/or consultants with experience in the local market to perform financial due diligence on site and/or gather independent information to validate the financial information provided by the company. Records might need to be converted into U.S. GAAP or International Financial Reporting Standards ("IFRS") to allow comparability and analyze the impact on future consolidations.

Businesses' and governments' interests	Investors should understand the relationship between the company and the state as companies are frequently supported or influenced by the state. Conflict of interest is a common issue in emerging markets and the instability that would be caused by a change in the relationship with the state is a risk that should not be underestimated. Personal relationships with these governments are key for some businesses and more often than not cannot be passed on to a new owner.
Unstable regulatory environment	Regulations in emerging markets can be complex and unstable. Often, emerging markets' legal systems move too slowly for enforcement which increases the risk of corruption and bribery. Adequate investor protection is often missed. Other areas of concern are future regulatory requirements in which emerging markets are highly uncertain and volatile. It is important to work closely with a trustworthy local law firm throughout the process.
Political environment	Political stability and elections are other factors investors should consider. Elections are a key indicator to project the political stability or trajectory of a jurisdiction. For example, Argentina had an election during 2015 and the new government has already shown a favorable change towards foreign investments in comparison to the previous government who was in power for 12 years and made foreign investments very difficult.

Investors need to be able to examine the financial viability of an investment in an emerging market. They will need to apply an integrated approach to ensure an appropriate risk assessment that will allow them to develop a strategy aligned with the emerging market reality. ■

Claudia Osmar is a partner at EisnerAmper LLP. For more information, feel free to contact her at Claudia.Osmar@eisneramper.com; 212.891.6907.

Alternative Investment Industry Outlook for Q3 and Beyond in 2016

By Elana Margulies Snyderman

INTRODUCTION

With the second quarter dominated by the Brexit vote, perhaps the biggest impact for the alternative investment industry which caused both immediate and longer-term uncertainty, investors are rethinking their upcoming alternative investment allocations on the heels of which strategies are expected to outperform; and which are expected to struggle. The views were mixed. Not surprisingly, Brexit inspired immediate investor interest in macro strategies, along with U.S. equities and real estate. Separate from Brexit, the outlook on equities-focused managers varied, with some slated to shy away from long/short generalists in favor of sector-focused and long-biased managers while others are on target to move away from long-biased. Others are looking at more esoteric hedge fund strategies including structured credit and direct lending, the latter being profitable when banks have scaled back on lending. And on the less liquid front, besides real estate, there is increased interest amongst various groups of investors in private equity and venture capital opportunities.

Other alternative investment trends predicted for this quarter and the remainder of 2016 include more launches planned for both hedge funds and less liquid funds, on the hedge fund front, long/short equities and specialty credit, and on the latter front, new real estate-related entities and venture capital technology focused funds.

And finally, the debate on fees, along with founders' share classes, is expected to persevere with investors continuing to negotiate for lower fees in their favor and managers expected to conform.

INVESTOR OUTLOOK

It is not surprising that the Brexit vote prompted investor interest in macro managers.

"Brexit seems to have increased interest in macro strategies, but it remains to be seen how large the actual inflows will be," said industry veteran Keith Danko, founding partner of Witherspoon Partners in Princeton, New Jersey.

He added: "U.S.-listed equities, especially large capitalization stocks, and U.S. real estate, again larger commercial properties, are still viewed as low-risk yet providing some minimum acceptable return. The U.S., rightly or wrongly, is still viewed as the best haven. Buying the U.S. and shorting anywhere else is a trade that has worked for 3 years now, and Brexit gave it another boost."

Additionally, EisnerAmper has heard that some investor groups, specifically family offices and funds of hedge funds, are transitioning away from long/short equity generalist managers due to underperformance and instead are favoring sector-focused and long-biased ones. The HFRI Equity Hedge Index confirmed the underperformance amongst long/short generalist managers since global equity markets in June posted steep losses following Brexit. It returned -0.27% in June and -0.16% for the first half of 2016.

Given the underperformance of global equity markets, investors are capitalizing on more niche strategies, including structured credit and direct lending, since these managers have been able to achieve positive returns amid low or halted interest rates.

However, the $270m endowment at Teachers College Columbia University is one investor who has moved away from long-biased managers in favor of smaller more hedged managers, and in addition, is favoring less liquid opportunities such as real estate and private equity.

"Our current exposure to marketable alternatives is about 28%, but is in the midst of a fairly substantial redeployment, away from very long-biased, larger cap oriented managers towards seasoned but smaller, much more hedged managers with a heavier tilt towards SMID equity," said Bruce Wilcox, chair of the Investment

Committee. "Our current NAV in non-marketable is 8% with a fairly heavy exposure to real estate and credit, but we have recent, as yet largely unfunded, commitments to secondary private equity and health care royalties that could double that exposure. We are very attentive to making sure we believe we are very well compensated for the illiquidity."

LAUNCH ACTIVITY

EisnerAmper has heard that anticipated launch activity for this quarter and the remainder of 2016 points to more fund debuts, specifically long/short equity including long-biased offerings; along with specialty credit; and on the less-liquid side, real estate and venture capital with a technology focus.

Frank Napolitani, director, national head of business development in EisnerAmper's Financial Services Group, said the firm continues to see the normal amount of long/short equity fund launches, but an increase in volume amongst specialty credit funds, which focus on funding leveraged buyouts ("LBOs"), Hollywood films, and emerging market high yield and stressed debt.

"Although the volume of new launch inquiries has remained steady, it will be interesting to see the number of funds that successfully secure the seed capital needed to begin operations," he said.

Todd Hankin, partner in the Financial Services Group in EisnerAmper's San Francisco office, added the West Coast is seeing an uptick in real estate launches and venture capital activity, specifically with a technology focus.

"We are seeing a significant amount of launch activity across real estate, likely due to the search for income and appreciation opportunities away from the richly valued securities markets," he said. "Opportunities range from holding actual real estate, buying or originating real estate loans, and investing in real estate related entities (e.g., technology or software or platforms in the real estate industry) to more creative ideas such as buying options on homes."

He added that there is a continued growth in the venture capital space, especially with a technology focus due to San Francisco's proximity to Silicon Valley.

FEES

The debate on hedge fund fees is expected to continue this quarter and beyond with the managers being more flexible on their fee structure in favor of the investors who request they negotiate to lower thresholds.

"We are certainly seeing more flexibility with fees, including more of the fee geared toward incentive and less toward management fees," said Jeff Parker, partner in EisnerAmper's Financial Services Group in New York. "We are also seeing special arrangements for certain investors, such as founders' share classes."

Ongoing recent published reports confirmed that the hedge fund industry standard 2/20 fee structure might not be as common going forward and will likely transition to 1.5/20.

CONCLUSION

For this quarter and the remainder of the year, investors and managers are still digesting the Brexit vote and how it will impact their respective portfolios and their performance. The general consensus is investor interest going forward is leaning toward more niche hedge fund strategies, and/or favoring less liquid investments over hedge funds given hedge funds have charged high fees for lack of performance; and are actively looking at real estate, private equity and venture capital. ■

Elana Margulies Snyderman is a senior manager in EisnerAmper's Financial Services Group. Questions? Contact Elana at elana.margulies-snyderman@eisneramper.com or 212.891.6977.

Cybersecurity Regulatory Risk: Where We Stand

By Venkat Rao

Cybersecurity is a topic that pre-occupies, and may even frighten, investment advisors and broker-dealers. High profile data breaches, such as the Panama Papers, have embarrassed prominent institutions and caused significant losses of confidential data, money and reputations. If that weren't enough, regulators waste no opportunities to hold organizations accountable when breaches occur. The unpredictable nature of this threat can overwhelm even the most sophisticated firms.

While meeting regulatory expectations can seem daunting, a closer look at the cybersecurity threat indicates that the regulatory risk can be mitigated with proactive management. For cybersecurity, recent SEC pronouncements indicate that blocking and tackling can go a long way to meeting regulatory expectations and mitigating cyber risk. To understand how to meet those expectations, it's important to review how the SEC has addressed cybersecurity over the past couple of years.

REGULATORY DEVELOPMENTS SINCE 2014

On April 15, 2014, the SEC's Office of Compliance Inspections and Examination ("OCIE") issued a Risk Alert announcing an examination sweep of investment advisors and broker-dealers to assess cybersecurity preparedness. Document requests during the sweep largely tracked the cyber risk framework published by the National Institute of Standards ("NIST"). After examining 57 broker-dealers and 49 investment advisors, the SEC published its examination sweep summary in February 2015. The following key observations have set expectations for firms' cyber practices:

- **Policies and Procedures/Business Continuity Planning:** The vast majority of firms (93% of broker-dealers and 83% of investment advisors) have adopted information security policies, and many address cyber impacts in business continuity plans.
- **Risk Assessments:** The vast majority of firms (93% of broker-dealers and 79% of investment advisors) conduct periodic firm-wide risk assessments, which include the identification of vulnerabilities to cyber-attacks.
- **Vulnerability to Attacks:** Most firms (88% of broker-dealers and 74% of investment advisors) reported being targets of cyber-attacks (e.g. fraudulent e-mails, phishing scams, employee misconduct) either directly or through their third party vendors.
- **Published Standards and Frameworks:** Most broker-dealers (88%) and over half of investment advisors (53%) utilized published cybersecurity risk standards, such as NIST, to model their information security architecture and processes;
- **Vendor Management:** Most broker-dealers (72%) have incorporated cyber risks into third party vendor contracts, but fewer investment advisors (24%) have done so.

What to make of these results? When viewed in the context of the SEC's core mission of investor protection, they come from the Commission's focus on firms' ability to protect customer/investor information through stronger controls. These themes became apparent in OCIE's 2015 cybersecurity examination initiative announced in September 2015:

Investment advisors and broker-dealers must realize that the SEC will continue to pursue these cases where cybersecurity controls are weak.

- **Governance and Risk Assessment:** Have advisors and brokers conducted a risk assessment to determine their exposure the cyber threats applicable to their business? Have firms utilized cybersecurity frameworks, such as NIST's, to determine their risk? Have risks been communicated to senior management and the board of directors for appropriate actions?
- **Access Rights and Controls:** Who has authorized access to the various parts of the firm's systems? Does the firm segment critical data to prevent access from unauthorized users? What type of encryption methodology does the firm employ? Is multi-factor authentication employed? How is remote user access addressed?
- **Data Loss Prevention:** How does the firm monitor transfer of data through emails or uploads? Are data or fund transfers reviewed for authenticity? Are proper controls in place to protect data and meet recordkeeping requirements (e.g., SEC Rule 17a-4)?
- **Vendor Management:** What are the firm's practices and controls related to the use of third-party vendors? Does the firm conduct adequate due diligence and oversight prior to engaging with the third parties? Is vendor management part of the firm's risk assessment process?
- **Training:** Are employees properly trained to avoid unintentional losses of data or exposing the firm's network to vulnerabilities? How often is the training conducted? Is training tailored to particular employees' duties? Has the firm incorporated incident response plans into training?
- **Incident Response:** Has the firm established policies and procedures, assigned roles, assessed vulnerabilities, and developed plans to respond to cyber breaches? Has the firm inventoried all data to determine the highest priority assets requiring protection?

Recently, the SEC has also proposed a new rule to require investment advisors to adopt written business continuity and transition plans ("BCPs"), which makes reference to cyber-attacks as a key risk. This development indicates a possible convergence between BCP and cybersecurity frameworks.

RECENT ENFORCEMENT CASES

Recent enforcement cases closely track the OCIE's pronouncements, as the Commission cited privacy rules under Regulation S-P to bring enforcement actions. In September 2015, the Commission censured and fined a St. Louis-based advisor for failure to establish cybersecurity policies, which preceded a cyber breach on a third-party site resulting in compromised personally identifiable information of approximately 100,000 customers. The SEC, citing a violation of Reg S-P, also noted the advisor's failure to conduct periodic risk assessments. Though no harm resulted to the advisor's clients, this case tracks the Risk Alert's reminder to (a) conduct periodic risk assessments; (b) implement data loss prevention measures; and (c) properly manage third-party vendors, as advisors are still responsible for data breaches occurring on third-party sites.

In April 2016, the SEC fined a New York broker-dealer $100,000 for violations of Reg S-P for failing to safeguard customer data through the improper use of email addresses and electronic fax accounts. Although not citing cybersecurity concerns directly, the Commission stressed that the broker-dealer failed to adopt policies and procedures reasonably designed to ensure the confidentiality and security of data, a primary purpose of the SEC's Risk Alert. As with the previous case, the fact that customers were not harmed did not prevent the enforcement action.

Cybersecurity Regulatory Risk: Where We Stand

Recently, the SEC has also proposed a new rule to require investment advisors to adopt written business continuity and transition plans ("BCPs"), which makes reference to cyber-attacks as a key risk. This development indicates a possible convergence between BCP and cybersecurity frameworks.

WHERE DOES REGULATION GO FROM HERE?

Investment advisors and broker-dealers must realize that the SEC will continue to pursue these cases where cybersecurity controls are weak. To prepare, the most effective steps to take include:

- **Conduct a cybersecurity risk assessment:** A complete review of a firm's cybersecurity policies and procedures should reveal any control deficiencies. Without such an assessment, no firm can be sure how best to prevent breaches of customer data.
- **Perform penetration and vulnerability testing:** Firms must understand the vulnerability of client/customer data before they can protect the information. The Commission has made clear from enforcement cases that failure to take adequate protection steps under Reg S-P will result regulation sanctions. Many advisors and brokers hire third parties to test the vulnerability of their networks to hackers.
- **Examine adequacy of policies and procedures:** Advisors and brokers often fail to establish and implement policies and procedures reasonably designed to prevent and detect non-compliance. Cybersecurity is no different. Compliance officers should work with their firm's chief information security officers ("CISOs"), or equivalent, to ensure information security and technology policies adequately address cyber risks.
- **Review business continuity plans:** The SEC's proposed rule suggests BCPs should incorporate cybersecurity disruptions. When testing a BCP's effectiveness, simulate scenarios where a cyber breach triggers the activation of an incident response plan.

Asset managers and broker-dealers should not wait for a cyber breach to take the aforementioned steps. ■

Venkat Rao is a director with EisnerAmper Global Compliance and Regulatory Solutions ("GCRS"). To discuss this article and other new regulatory initiatives, you can reach Venkat at 347.735.4761 or venkat.rao@eisneramper.com.