I am delighted to welcome you to the first edition of the quarterly Willis Financial Institutions Group (FIG) Asset Manager newsletter.

In this first edition Willis experts look at how recent Financial Conduct Authority reviews and enforcement actions are impacting the asset management sector in the UK. We also review the SEC’s concern with cyber risk and the “systemic importance” of asset managers in the US.

FIG is a new industry group at Willis. It comprises ex-bankers, former regulators and insurance professionals. FIG has been specifically created to connect experience across the Willis Group and to support our clients with the resources they need to respond to changing regulatory pressures and uncertain economic and market conditions. As a risk advisor and as a broker, we work with clients to identify and develop solutions to their risk management problems. FIG will help bring the best of Willis to our clients.

FIG’s client proposition consists of three pillars:

**INFORM:** Our unique experience enables us to assist in identifying and overcoming key regulatory and commercial challenges.

**PROTECT:** We create effective and reliable risk mitigation solutions using insurance and non-insurance markets.

**GROW:** We optimize our client’s commercial position by freeing up capital and growing revenue, thus enabling clients to enhance their own business strategy.

Please contact me or your usual Willis representative if you’d like to share your thoughts and feedback or if you’d like further information about how FIG can work with you.

Thank you for your time and I hope you find this newsletter informative.

Mary O’Connor
CONTENTS

FCA enforcement action is creating new regulatory risks for asset managers ........................................... 4
Asset managers must take responsibility for their outsourcing .................................................................. 6
Behavioral economics can help you better understand your clients ............................................................ 8
Do asset managers contribute to systemic risk? ........................................................................................... 10
Safeguarding asset managers against mounting cybersecurity threats ......................................................... 12
FCA ENFORCEMENT ACTION IS CREATING NEW REGULATORY RISKS FOR ASSET MANAGERS

In April 2014, the FCA imposed a penalty upon Invesco Asset Management and Invesco Fund Managers (Invesco) of £18.6m for failings in fund management. The Invesco case highlights two regulatory risks potentially facing the wider asset management community – conduct risk and financial penalty risk.

The Invesco Case
The FCA found that Invesco was guilty of breaching two principles of the FCA’s Principles for Business:

- Principle 7 - firms should communicate in a way that is clear, fair and not misleading.
- Principle 3 - firms should have appropriate systems and controls in place.

Invesco’s breaches spanned a period of four years, from May 2008 to November 2012, and impacted primarily retail investors. Although the Invesco case continues the FCA’s focus on the asset management sector, Invesco was not fined for client money failings like other asset managers. The Invesco case highlights new regulatory risks potentially facing the wider asset management community – conduct risk and financial penalty risk.

Conduct Risk
The FCA’s conduct risk agenda is taking shape and is concerned with the extent to which a firm ensures its clients and market integrity is at the center of way it conducts business. Conduct risk impacts the delivery of a fair customer outcome and the fair outcome itself.

Invesco’s failure to adequately disclose information to investors should be seen through the FCA’s “conduct risk” framework. For example, Invesco disclosed the use of derivatives in its materials to investors but did not adequately reflect the impact and risks arising from the use of derivatives. In another instance, a simplified prospectus failed to disclose...
adequately to investors that Invesco could invest funds in derivatives although the full prospectus provided for their use. Consequently, the FCA held that some investors were not fully aware of the risks involved when investing their money.

*Although this may seem draconian, the FCA is concerned that inadequate disclosure meant that investors may have been exposed to greater levels of risk than they otherwise would have accepted. The inadequate disclosure affected the delivery of a fair outcome to investors.*

Similarly, the FCA concluded that Invesco's inadequate systems and controls resulted in a failure to record trades on a timely basis and monitor the allocation of aggregated trades. Outdated systems have the potential to cause consumer detriment, unfair treatment and loss to consumers. This falls squarely within the FCA's conduct risk agenda because the outcome itself may not have been fair to consumers.

*Management of conduct risk will require risk analysis, risk mapping and additional resources. As the FCA becomes increasingly proactive and forward-looking, firms must identify their risks now, before risks are identified for them in the context of an investigation.*

**Financial Penalty Risk**

As we move further away from the old penalty regime, asset and fund managers facing regulatory investigation may find themselves at the receiving end of a significant financial penalty due to the determination of “relevant revenue” under the new penalty regime. The Invesco penalty was calculated using a combination of the old and new penalty regime. The FCA applied the old regime to breaches occurring before 6 March 2010 and the new regime to breaches occurring after that date.

**New Penalty Regime**

The new penalty regime is a five-step process starting with disgorgement of any profits made from the breach. Step two is the determination of a figure that reflects the seriousness of the breach, derived from “relevant revenue” which is usually the revenue generated by a firm from a particular product line or business area. The FCA concluded that “relevant revenue” comprised relevant management fees of the affected funds together with the portion of the initial charges not rebated to customers from the affected funds during the period of the breach.

This assessment resulted in “relevant revenue” of £690 million for Invesco from which the FCA took 5%, to reflect the low seriousness of the breach. The resulting figure of £34.5 million was reduced to £21.6 million because the FCA concluded the breaches were not indicative of widespread failings and all losses to the funds had been fully reimbursed by Invesco. There was a further discount of 30% for early settlement.

**Old Penalty Regime**

In contrast, the old penalty regime, which had a simpler methodology, led to a financial penalty of £5 million. This was reduced to £3.5 million once the 30% discount for early settlement had been applied.

The final penalty of £18.6 million combined the old and new penalty figures.

Invesco was fortunate that its breaches were not indicative of wide systemic failings. Other asset managers, working with legacy systems and improper systems and controls, may not be as fortunate and will not receive as large a discount. As we move away from the old penalty regime, the determination of “relevant revenue” under the new penalty regime will result in ever greater penalties for asset managers.

*July 2014*
The FCA’s concern with outsourcing risk is driven by its “consumer protection” objective. In October 2013, the FCA held its annual Asset Management Conference; outsourcing formed part of the agenda. This should not have been a surprise. Towards the end of 2012, the FCA’s predecessor, the FSA, had issued a “Dear CEO” letter setting out its expectations of asset managers that outsource critical activities and reminding asset managers that while they may outsource a function, they cannot outsource their responsibility for that function.

The FSA was concerned about two areas of risk:

1. **Resilience Risk**
   - If an asset manager’s service provider was to suddenly fail and therefore be unable to provide their services for an indefinite period, the asset manager would not be able to continue to provide the service for its customers, which could result in detriment to customers.

2. **Oversight Risk**
   - If an asset manager failed to oversee their service providers effectively, it could result in poor outcomes for customers.

The thread running through resilience and oversight risk was the FSA’s concern with the potential detrimental impact upon consumers.

The FCA has continued this focus and published the results of its outsourcing review in November 2013 (“Outsourcing in the Asset Management Industry: Thematic Project Findings Report”). It concluded that asset management firms were not adequately prepared to respond to, and mitigate “resilience risk”. The contingency plans that firms had in place were inadequate, ineffective or impractical.
Some asset managers did not even have contingency plans in place because they took the view that since their service providers were part of the systemically important banking groups that were too big to fail, the government would offer a bail-out!

Customers will also not be pleased to learn that some asset management firms are “outsourcing” resilience risk by relying upon the government to use taxpayers’ money to bail out large financial institutions that provide outsourced services to asset managers. An asset manager’s customer can be taxpayers too, and this stance is hardly evidence of protecting consumers or complying with SYSC 8 of the FCA’s Handbook. As the FCA reminds us, a function can be outsourced, not the responsibility.

In relation to “oversight risk”, the FCA noted that asset managers generally accepted responsibility for critical outsourced activities due to the accompanying reputational risk they would suffer if the service provider failed. However, depending on the outsourced activity, the way in which oversight was exercised was inconsistent, inadequate and infrequent, with service-level agreements not being reviewed regularly. Asset managers should carefully consider the FCA’s findings.

The Outsourcing Working Group formulated a series of principles to respond to the issues identified by the FCA, from firms having a better understanding of the scope and nature of the services being outsourced, to firms developing an exit plan in the event of outsourcing failure. These principles put responsibility for outsourcing back upon asset managers, where the FCA, and customers, would expect it to be.

Understanding Outsourcing Risk
The FCA’s outsourcing review should prompt asset managers to re-evaluate their operational risks. Not only does this meet regulatory requirements (FCA’s SYSC 8 [“Outsourcing”]) and advance the FCA’s “conduct risk” agenda, it makes simple commercial sense too.

Asset managers should consider their outsourced services, such as IT systems, supply chain and business continuity measures and ask:

— For how long has the service been provided by the incumbent?
— When did the last competitive tender take place?
— Are service-level agreements reviewed and audited regularly?
— Who is responsible for conducting detailed and on-going due diligence on service providers?

Extra diligence should be exercised where client assets are involved; the regulator has a track record of fining asset managers in connection with client money failings.

By asking these questions and challenging the incumbent outsource provider, asset managers will slowly create and improve competition in the outsourcing market, achieving cost efficiencies and value for shareholders.

Once asset managers understand their outsourcing and related operational risks, chief risk officers and heads of compliance will be able to effectively mitigate the risks, through insurance-based solutions, improvements in systems and controls, or a combination of the two. In either case, the asset manager will have identified the risk, which is the first step in fulfilling regulatory requirements and putting customers at the heart of their businesses. The FCA’s outsourcing review shows that some asset managers have yet to take the first step.

A Role for the Insurance Broker?
Insurance brokers have a potential role to play in this process to the extent that they include risk mapping and operational risk assessment as part of their services.

Risk mapping and risk assessment is a collaborative and consultative process with clients. In its initial stages, this form of risk management involves a dialogue between the client and risk advisor to identify and profile the nature and causes of perceived risks. Identified risks are then mapped against existing insurance to identify potential exposures, which might be mitigated through improvements in policy language or through additional insurance products.

Effective operational risk assessment should also consider ‘quantification of maximum impact’ and ‘frequency of loss’ scenarios to ensure an accurate quantification of the frequency and the depth of impact of the risks identified by risk mapping exercises.

Together, effective risk mapping and operational risk assessment provide the basis for identifying, managing and mitigating risk, including the outsourcing risks identified by the FCA.

From a regulatory perspective, effective risk mapping and operational risk assessment can provide senior management with a quantifiable and evidential basis to demonstrate effective management of outsourcing risks to their FCA supervisors.

July 2014
Behavioral economics applies psychological insights into human behavior to investigate how people make economic decisions. Understanding the constraints and influences that your clients face when making investment decisions can help you become a more informed advisor.

The FCA came into effect on 1 April 2013 and one of its very first acts was to release a 70-page paper entitled “Applying behavioural economics at the FCA”. Behavioral economics suggests consumers are not rational, logical market participants but subject to behavioral biases which influence their preferences, beliefs and decision-making. Biases can lead to misjudgment and inconsistency which can cause individuals to make mistakes when selecting financial products, even though they are in possession of disclosed information that should enable them to make good and informed choices.

The FCA has highlighted examples of biases upon consumer purchases. Firstly, an individual's preferences may be moved by emotional factors. A consumer may seek to avoid regret by purchasing a type of insurance he does not need, or he may borrow excessively to purchase products without considering his ability to repay the loan.

Biases can affect an individual's beliefs. Consumers are often overconfident in their own decision-making ability which can affect purchasing and investment decisions and cause clients to fail to properly assess risk. Consumers will recall an investment loss more than an investment gain, placing undue emphasis on the former, which may dictate their reaction to future losses, including the length of time they hold a loss-making position.

Biases can also affect a consumer’s decision-making. Consumers might adopt a rule of thumb for decision-making, picking the most familiar option of a product or basing a decision on whether they trust the sales advisor. Consumer decision-making can also be affected by the way information is disclosed or framed.
Upon the paper’s release, Martin Wheatley, the current chief executive of the FCA, stated:

“We want the regulatory system to use behavioural economics to ascertain whether people are being put off switching products through inertia, inattention or even the simple fear of regret from making a wrong decision.”

Since the paper’s release, the FCA has been relatively silent about providing guidance on behavioral economics and how it applies to firms. It has though recently released a study examining how the sale of insurance add-ons affected consumer decisions.1 The study was the FCA's first experience of using experimental methods to investigate consumer behavior.

The FCA’s study demonstrated that the structure of the transaction affected consumers. For example, greater complexity of comparing offers from different providers led to a deterioration in consumer decision-making – consumers were less able to identify the best deal and lost money. The study also showed that lower transparency, due to add-ons being revealed only at the point of sale significantly exacerbated poor consumer outcomes. Also, the presentation of pricing information had the potential for an adverse effect on consumer behavior.

Some of the study’s findings have parallels to the FCA's recent comments over dealing commission, bundled charging and the lack of transparency within the asset management sector. The FCA will continue to look closely at the role of bias, its influence upon consumers, firm behaviour and its potential impact upon competition.

Although daunting, firms may want to use behavioral economics as an opportunity to better understand their clients. If advisors are able to understand these biases, they may be better able to question the client, better identify his attitude to risk and reward and better understand his investment objectives. This is likely to improve the overall relationship between the client, firm and advisor.

July 2014

In September 2013, the US Department of the Treasury’s Office of Financial Research (OFR) issued its report called “Asset Management and Financial Stability” (OFR Report) which looked at how asset management firms and their activities could “introduce vulnerabilities that could pose, amplify, or transmit threats to financial stability.”

The OFR Report studied the range of asset management activities and suggested that these activities as a whole made them systemically important and a potential risk to financial stability. In reviewing the various activities performed by asset managers it stated that these activities:

“...could create vulnerabilities— if improperly managed or accompanied by the use of leverage, liquidity transformation, or funding mismatches.”

The OFR report, which was commissioned by the Financial Stability Oversight Council (FSOC), itself established by the Dodd-Frank Act 2010, was widely criticized. Senators claimed the OFR Report contained numerous inaccuracies and urged the Department of the Treasury to distance itself from the OFR Report, lest it tarnish the Treasury’s reputation. The Investment Company Institute (ICI), an industry body, wrote a 41-page letter to the SEC highlighting numerous shortcomings within the OFR Report, including errors such as:

— Problems with methodology, data, and the presentation of information
— Loss of the key distinction between banks and asset management firms - the agency nature of an asset manager’s business, which results in a vastly different risk profile
— Failure to recognize that the existing regulation of registered funds and their advisors not only protects investors but also mitigates risk to the financial system

Many others poked holes after the SEC invited public feedback on the OFR Report.
Despite the criticism of the OFR Report, the question over asset manager designation as systemically important financial institutions (SIFIs) has not receded. In Europe, the Financial Stability Board (FSB) and the International Organisation of Securities Commissions (IOSCO) issued a consultation document entitled “Assessment Methodologies for Identifying Non-Bank Non-Insurer Global Systemically Important Financial Institutions (NBNI G-SIFIs)”. The consultation document explained how the financial distress or disorderly failure of a NBNI could be transmitted to other financial entities and markets, thereby posing a threat to global financial stability. The consultation document did not propose that any specific entity be designated as a NBNI G-SIFI, or describe a policy that might apply to them.

The consultation document recognized that NBNI financial entities often have very different legal forms, business models and risk profiles. Any methodology for identifying NBNI G-SIFIs would have to be applicable to the wide range of NBNI institutions. It proposed introducing a basic set of impact factors to be applied to all NBNI financial entities:

- Size
- Interconnectedness
- Substitutability
- Complexity
- Global activities

The consultation document also recommended materiality thresholds to determine SIFIs of:

- Investment Funds: $100 billion in net assets under management for investment funds.
- Hedge Funds: $400-$600 billion (or more) in Gross National Exposure.

Many organizations and entities responded to the consultation document. Some challenged “size” and assets under management for determining systemic risk and importance. The industry bodies highlighted the importance of leverage as posing a greater systemic risk, whilst others reiterated the crucial role of an asset manager in taking financial risk out of the traditional banking system, thereby aiding financial stability, not endangering it. The asset management industry also articulated the potential negative effects of a G-SIFI designation upon an asset manager, its funds and investors. Most of these responses mirrored concerns previously made by asset managers in the US.

Against this debate, the FSOC hosted its Asset Management Conference in May, during which it discussed potential risks to US financial stability. Perhaps mindful of the ongoing concerns, Mary Miller, the Under Secretary for Domestic Finance at the Treasury, spoke about the importance of the FSOC analyzing the asset management industry to determine whether they pose any risks to US financial stability, but stressed that there was “no pre-determined outcome”. There was also recognition of the need for greater transparency and disclosure when making such important decisions.

The question of asset managers being designated G-SIFIs is unlikely to be resolved this year. The criticism of the OFR Report, a similar ongoing debate in Europe, and recognition by regulators of the need for increased communication with its stakeholders, may have pushed aside the regulator’s desire for a swift decision. If FSOC is to designate an asset manager for SIFI status, it is very likely this will occur in 2015. Before any decision is taken however, it seems that the FSB and IOSCO will release a second consultation document in the fall. This will fuel and inform the debate on both sides of the Atlantic for the remainder of this year.

July 2014

---

1 Asset Management and Financial Stability, September 2013, Office of Financial Research, page 1  
2 http://www.reuters.com/article/2014/01/24/us-financial-regulation-asset-idUSBREA0NILG20140124  
3 www.ici.org/pdf/13_ici_ofr_asset_mgmt.pdf, dated 1 November 2013
On 15 April 2014 the Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations (OCIE) released a cybersecurity initiative risk alert announcing it would be examining 50 registered broker-dealers and investment advisors to assess their cybersecurity preparedness. The announcement was accompanied by a seven-page sample request (OCIE Sample Request) for information and documents.

A “Global Threat”
The OCIE Risk Alert followed on from the SEC’s roundtable on cybersecurity, held on 26 March, which acted as a forum for the SEC, other agencies and market participants to discuss cyber risks and better understand how to combat them. The roundtable’s agenda comprised four topics: cybersecurity landscape, public company disclosure, market systems and broker-dealers, and investment advisors and transfer agents.

In her opening statement, SEC Chair Mary Jo White expressed concern about the growing threat to the US financial system, global institutions and consumers from cyberattacks and hackers:

“This is a global threat. Cyber threats are of extraordinary and long-term seriousness. They are first on the Division of Intelligence’s list of global threats, even surpassing terrorism.”

The OCIE’s Risk Alert is designed to “assess cybersecurity preparedness in the securities industry and to obtain information about the industry’s recent experiences with certain types of cyber threats.” The OCIE’s Sample Request comprises 28 questions covering five main areas:

— Identification of risks/cybersecurity governance
— Protection of firm networks and information

This article was produced for the Financial Institutions Group’s Asset Manager Newsletter and was authored by:

Jagdev is the Director of Risk & Regulatory Strategy within the Financial Institutions Group at Willis. He regularly advises clients on financial regulation, emerging risks and trends.

Prior to joining Willis, Jagdev worked in the Enforcement and Financial Crime Division of the Financial Services Authority (now Financial Conduct Authority), investigating investment banks and senior directors and officers within the financial services industry.

Before joining the FSA, he specialized in International Arbitration, Dispute Resolution and Litigation at a law firm in the City of London.
— Risks associated with remote customer access and funds transfer requests
— Risks associated with vendors and other third parties
— Detection of unauthorized activity

Issues for Asset Managers
Asset managers will probably be familiar with some of the questions on the OCIE’s Sample Request, such as requests for copies of written security policies and information about regular testing. However, there are some other questions which provide insight into the SEC’s thinking and which asset managers should act upon now to improve their resilience to cyber risks:

— Does the firm have a dedicated person, such as a chief information security officer, responsible for cybersecurity?
Some asset managers will probably not have a dedicated person dealing with cybersecurity issues. Cyber risk issues tend to fall to the compliance officer, risk officer, head of information technology or a combination of these people. As such, the issue is unlikely to be top of the priority list, or it might be unclear who has overall responsibility.

Asset managers should ensure there is clarity about who takes ownership for the effective management of cyber risk. If possible, this should be a dedicated individual, with the necessary qualifications and skills. If a single individual is not appropriate due to the asset manager’s relative size, senior management should ensure cyber risk is managed by someone with sufficient engagement and resources to give the matter the priority the SEC has deemed.

— Does the firm restrict access to data, systems and information to authorized personnel only?
Many asset managers’ passwords protect their systems but use a single universal password which, once entered, will provide unrestricted access to a range of IT systems. Other firms utilize multiple IT systems which do not communicate properly with each other, making it hard to properly audit, monitor and restrict access.

Asset managers should review this issue and ensure access is properly restricted; the rule of thumb should be that access to a system is restricted to an employee unless there is a well-documented business reason to grant access to a particular system.

— Does the firm maintain protection against Distributed Denial of Service (DDoS) attacks?
A DDoS attack attempts to shut down an online service by overwhelming it with traffic from multiple sources. Small sites are particularly vulnerable to DDoS attacks as they are not built to cope with significant traffic. However, larger online sites should not think they are immune. In recent years, several high profile companies have been the subject of DDoS attacks. In early July at least eight top Norwegian companies including financial institutions and insurance companies were targeted in what appeared to be co-ordinated cyberattacks.3

Asset managers should ensure they have robust online systems to guard against this kind of cyberattack, and proper contingency plans in place in the event of a DDoS attack. These measures should be regularly tested and updated to keep pace with evolving threats.

— Does the firm maintain insurance that specifically covers losses and expenses attributable to cybersecurity incidents?
Cyber insurance is no longer seen as optional, but an essential part of a firm’s cyber risk management and cyber resilience. Traditional insurance policies, such as general liability, will probably prove insufficient to effectively respond to the cyber threats identified by the SEC. The OCIE’s Sample Request demonstrates that the SEC believes cyber threats can emerge from multiple sources, including from outsourced activities and third-party providers.

Asset managers should consult with specialist insurance brokers to perform a cyber risk assessment and gap analysis to identify these cyber risks and exposures. Specialist insurance brokers can then ensure the asset manager and its clients are appropriately covered and protected in the event that they fall victim to a cyberattack. Appropriate cyber insurance protection will not stop a cyberattack but may prove to be the decisive factor in ensuring an asset manager swiftly recovers and limits the impact upon its sales, revenue, customer trust and reputation.

July 2014

1 Opening Statement at SEC Roundtable on Cybersecurity, Chair Mary Jo White, 26 March 2014, http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468#.U8EN20DwHq4
FINANCIAL INSTITUTIONS GROUP
GLOBAL FIG CONTACT DETAILS

GLOBAL LEADERS

Mary O’Connor
Global Head of Financial Institutions
+44 (0)20 3124 8991
mary.oconnor@willis.com

John Brosnan
Global Head of Sales
+44 (0)20 3124 6427
john.brosnan@willis.com

Jagdev Kenth
Director of Risk & Regulatory Strategy
+44 (0)20 3124 8560
jagdev.kenth@willis.com

REGIONAL LEADERS

Richard Magrann-Wells
US Co-Regional Leader
+1 212 915 8357
richard.magrann-wells@willis.com

Jonathan Bush
UK Regional Leader
+44 (0)20 3193 9495
jonathan.bush@willis.com

Zakia Campbell
US Co-Regional Leader
+1 212 915 8548
zakia.campbell@willis.com

Silvi Wompa
Western Europe Regional Leader
+4 684 638 926
silvi.wompa@willis.com

Natalia Char
Latin America Regional Leader
+57 (1) 606 7575
natalia.char@willis.com

Alexander Van Kuffeler
CEMEA Regional Leader
+44 (0)20 7558 9281
avkuffeler@willis.com

Tony Mitchell
Asia Regional Leader
+65 6591 8055
tonym@willis.com

George Harding
Australasia Regional Leader
+61 2 9285 4091
hardingg@willis.com