



# GLOBAL REGULATORY OUTLOOK

# 2017

---

## VIEWPOINT 2017

Opinions on global financial services regulation and industry developments for the year ahead

# Contents

- 04 Executive Summary
- 06 Who is the Regulator?

## 08 Brexit

- 10 Post-Brexit Models under AIFMD
- 12 Navigating the MiFID II Maze
- 14 What to Expect from Trump
- 16 Draining the Swamp?
- 18 No Right Answer

## 20 Cybersecurity

- 22 No Simple Exercise
- 24 The Convergence of AML and Cybersecurity
- 26 Preparing for and Responding Effectively to Cyber Attacks

## 28 Individual Accountability

- 30 Having an Impact - Senior manager regimes in the UK and elsewhere
- 32 The SFC's new "Managers-in-Charge" Regime: it's getting tougher at the top
- 34 The "Manager-In-Charge" Regime and Individual Accountability
- 36 U.S. Perspective on Enforcement Culture/Individual Accountability

**Julian Korek**, Duff & Phelps

**Julian Korek**, Duff & Phelps

**Killian Buckley and Alan Picone**, Duff & Phelps

**Nick Bayley**, Duff & Phelps

**Rosemary Fanelli**, Duff & Phelps

**Norm Champ**, Kirkland & Ellis

**David Larsen**, Duff & Phelps

**Adam Menkes**, Credit Suisse

**Sharon Cohen Levin**, WilmerHale

**Jason Elmer**, Duff & Phelps

**Monique Melis**, Duff & Phelps

**Tim Mak and Wings Turkington**,  
Freshfields Bruckhaus Deringer

**Nick Inman**, Duff & Phelps

**Polly Greenberg**, Duff & Phelps







### **About the Global Regulatory Outlook**

Our fifth annual Global Regulatory Outlook, provides a unique, global perspective on financial services regulations. This Viewpoint report outlines how professionals in the financial services industry see regulation impacting their industry in 2017.

Our research gauges perceptions on the key regulatory developments and the issues they pose for businesses. Throughout, Duff & Phelps experts provide perspectives and practical guidance on the key themes for the year, and beyond.

For further and more technical guidance, our Insight supplement outlines the specific, key regulations, requirements and deadlines by jurisdiction applicable to the asset brokerage and fiduciary industries.

We would like to sincerely thank all the professionals who took part in the survey and those who contributed their perspectives to the Global Regulatory Outlook reports. We hope they will help the industry face the year ahead with confidence.



**Author**

**Julian Korek**

Managing Director and Global Head of Compliance and Regulatory Consulting

Duff & Phelps

julian.korek@duffandphelps.com

## Executive Summary

Old challenges for financial services compliance are going to have a new relevance in our changing world.

We've seen the shock of the Brexit vote, the victory of Donald Trump and the rise of populist parties across the developed world. For many financial services professionals however, it's business as usual.

Our 2017 Global Regulatory Outlook (GRO) survey of 181 professionals shows they continue to contend with well-established challenges around competitiveness, international coordination and costs. Almost nine out of ten (89%) believe regulations are increasing costs, for instance, and compliance spending at a typical firm is expected to double in the next five years.

Today, the most common spend on compliance among asset managers, brokers, banks and others is up to 4% of revenue. By 2022, it's expected to rise to up to 10%. The proportion putting their compliance spending at less than 1%, meanwhile, is expected to halve.

### Technology trials

Spending on cybersecurity will account for at least some of this hike, and this has been a key development in the past year. After attacks on the Swift payment system,<sup>1</sup> the "unprecedented" theft from a UK retail bank's online accounts<sup>2</sup> and a huge increase in reported attacks on financial services groups generally,<sup>3</sup> regulators are widely expected to focus on firms' cyber defences and – and perhaps most crucially – their detection and response plans.

So far, regulators such as the U.S. Securities and Exchange Commission (SEC) have held off mandating precise requirements around cybersecurity. Nevertheless, about two-thirds of professionals in our survey expect it to be among the regulators' top three priorities in 2017. Only Anti-Money Laundering (AML) and Know Your Customer (KYC) to be among the regulators' top priorities.<sup>4</sup>

In any case, firms are taking this seriously; 86% say their company intends to put more resources and time into cybersecurity in the coming year. Other areas likely to see attention, meanwhile, are MiFID II, where more than half (54%) of those to whom it applies say they are still unsure if they're on track to comply by 3 January 2018; and the SEC's proposed rules to enhance information reported by investment advisors in 2017, which 62% of regulated firms say will impact them.

Most respondents (61%) concede that regulations will improve internal controls. More than half (54%) also say making executives and senior managers responsible for the actions of employees within the firm has a positive impact on the industry.

1 <http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD>

2 According to FCA chairman Andrew Bailey <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/financial-conduct-authority-november-2016/oral/42882.html>

3 <https://www.ft.com/content/66c95bc0-71b8-3adc-9e35-bef3e67b9292>

4 <https://www.bloomberg.com/news/articles/2016-11-10/trump-s-transition-team-pledges-to-dismantle-dodd-frank-act>





### **Bang for buck?**

More widely, however, scepticism about the value financial regulation brings remains. More than half say financial services regulation has either had little effect (35%) or actually worsened market stability (17%) – presumably reducing liquidity in some markets – against only 43% who say it has increased stability. Similarly, half (51%) say it has done little to improve investor confidence, and 7% say it has eroded it.

Finally, just one in ten says regulatory changes over recent years have adequately created safeguards to prevent a future crash.

This comes as no surprise: the findings are not vastly different to previous years. But scepticism regarding the efficacy of financial regulations since the crisis has added import in light of the recent political upsets in the U.S. and, perhaps, the UK.

In the former, the new president has pledged to “dismantle” Dodd-Frank, a position his Democratic opponent on the campaign trail, Hillary Clinton described as “reckless.” That disagreement foreshadows the opposition President Trump will face if he does push for any significant reduction in financial services regulation.

In this context, it’s interesting to note that financial services professionals themselves remain far from convinced that regulation – despite the vast costs imposed on the industry – has made markets safer.

### **A new world**

A similar observation may also apply in the UK if Brexit sees an end to EU passporting and enables the UK to determine its own, potentially lighter, regulation. In any case, most firms expect Brexit to have some impact on their compliance arrangements, whether in the

long term, over 18 months (26%); nearer term, within seven to 18 months (22%); or, in some cases, sooner (12%).

Confidence in the UK’s position as a financial centre is weak, however. Today it alone challenges New York as the pre-eminent global financial centre, with 36% naming it compared with 58% naming the U.S. city. Asked what location will dominate in five years’ time, however, the proportion naming New York remains steady, while those naming London more than halves to just 16%.

It’s a reminder, perhaps, of just how much uncertainty remains as we enter 2017; and it’s a reminder, too, if one is needed after the past year, that we cannot take anything for granted.



**Author**

**Julian Korek**

Managing Director and Global Head of Compliance and Regulatory Consulting

Duff & Phelps

julian.korek@duffandphelps.com

## Who is the Regulator?

Firms are increasingly coming under the authority of multiple regulators at home and abroad. That is creating challenges for those responsible for managing regulatory risk.

We've come a long way since the 1970s, when financial services industries across the globe were largely self-governing. Public pressure for greater accountability, transparency and trust has seen a proliferation of regulators and former industry bodies consolidating into government agencies. In the UK, for instance, the Financial Services Authority (now the Financial Conduct Authority) incorporated the IMRO (Investment Management Regulatory Organisation), SFA (Securities and Futures Authority) and PIA (Personal Investment Authority), as well as sections of the Bank of England.

This boom in state-sponsored regulation has coincided with enhanced cross-jurisdictional and regulatory collaboration, as well as high fines for regulatory failings.

Firms now find themselves subject to penalties and sanctions from multiple regulators and law enforcement agencies

for a single breach, with fines based on various, and often unclear, criteria. One international bank in 2012, for example, paid \$340 million to the New York State Department of Financial Services – a relatively new regulator in New York – and a day later \$327 million to the Federal Reserve. The same year saw U.S. authorities impose large fines on not only U.S. based firms but also UK institutions.

**With great power comes great responsibility**

This is, in part, why it's no surprise our survey shows nine out of ten in financial firms expect the cost of compliance to rise. But at some point that means we must question whether the industry and shareholders – and the wider public who ultimately pays – can continue to bear the burden of increasing regulation.

Brexit may allow for UK regulators to rethink and slim down the UK regulatory

landscape, particularly for institutional businesses. The same possibility can be seen in the U.S., where President Trump has already stated he believes that Dodd-Frank went too far and delayed economic recovery.

In the meantime, the utopia of a single global regulator is unlikely ever to be more than a dream, but regulators can continue to work across agencies and with firms to ensure the industry remains competitive, while still safeguarding against failures in the markets they oversee. And as regulatory change and political and economic upheaval continue, firms, too, should be ready. They need to be putting in place a global regulatory recovery plan to protect themselves from – or capitalise on – the changing regulatory landscape.

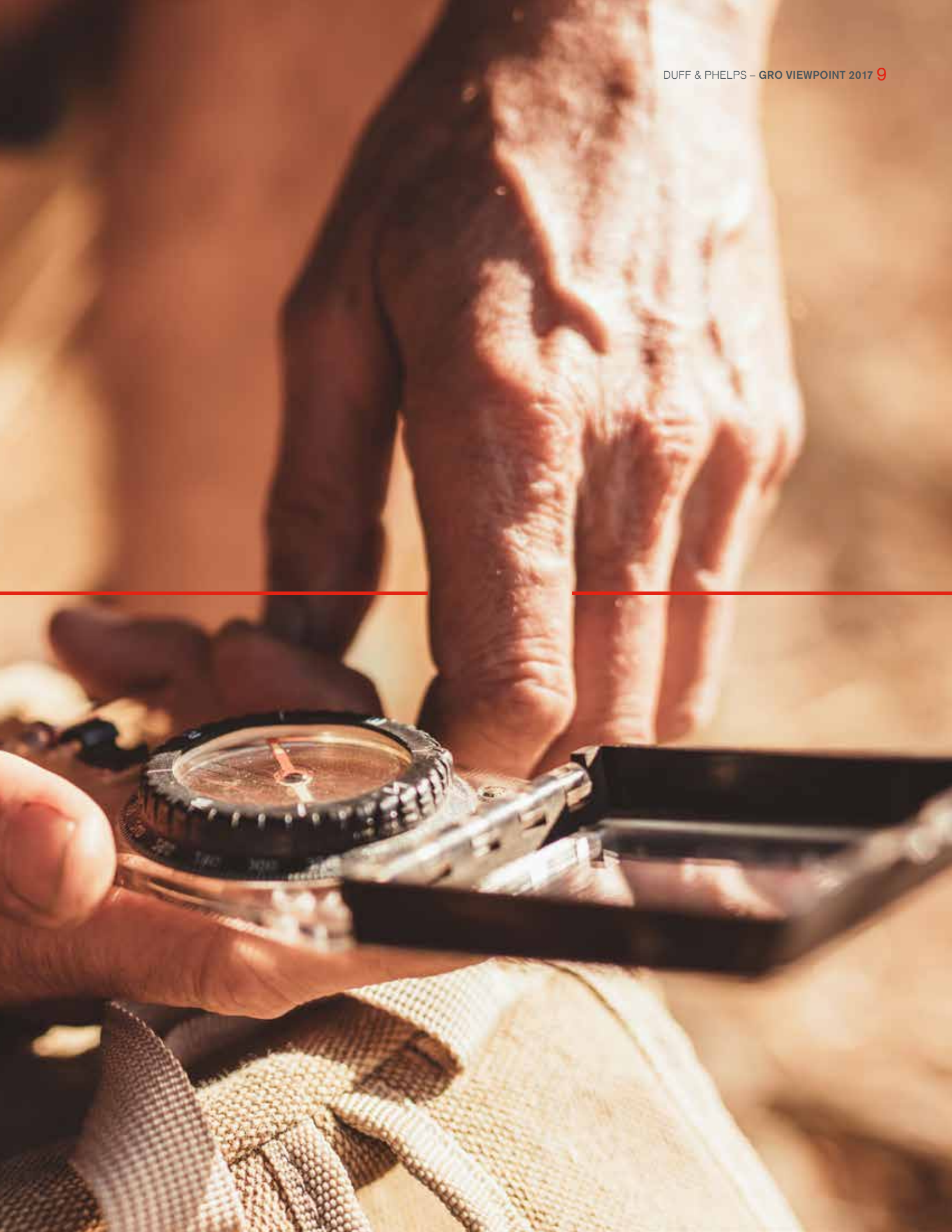




# BREXIT









**Authors**

**Killian Buckley**

Managing Director  
Regulatory Consulting  
Duff & Phelps  
killian.buckley@duffandphelps.com



**Alan Picone**

Managing Director and Global Head  
of Risk Consulting Practice  
Duff & Phelps  
alan.picone@duffandphelps.com

## Post-Brexit Models under AIFMD

Since it came into effect in 2013, the Alternative Investment Fund Managers Directive (AIFMD) has had a profound impact on funds' risk management. It's seen the role of risk management expand to encompass every part of the value chain, from portfolio risk to operational risk and liquidity.

This has required a cultural shift. Managers have had to take an ex ante – rather than ex post – approach: embedding risk management firmly into portfolio decision-making at the outset, rather than simply measuring potential impacts of decisions that have already been made.

Now, with Brexit looming, AIFMD could be about to change everything for British alternatives managers once again.

**Losing access**

Under the directive, asset managers must have an EU presence to take advantage of the marketing passport that allows funds to be distributed freely across Europe. With many expecting a 'hard Brexit' in which the UK is no longer a member of the European Economic Area, expectations that passporting will be fully protected appear to be fading.<sup>1</sup>

According to European Securities and Markets Authority (ESMA), there are no significant obstacles impeding the application of the AIFMD passport for a number of non-EU jurisdictions, including Canada, Guernsey, Japan, Jersey and Switzerland.<sup>2</sup> It can only advise, however. Ultimately any decision will be made by the European Commission, Parliament and Council.

Should UK-registered alternative investment fund managers lose their passporting rights, they will effectively be in the same position as U.S. managers and others outside the EU. If they wish to market to investors within it, they must come to another arrangement.

**Model opportunities**

One option will be to set up a legal presence in a jurisdiction such as

Luxembourg or Dublin. The requirements for adequate substance to prove genuine domicile are not light, however. UK managers already know the demands AIFMD puts on an organisation and may balk at the resources needed to locate core functions and skilled people outside the UK, as well as commit the minimum capital required.

It seems likely, therefore, that some will look to third-party management companies – as U.S. managers have done – rather than setting up their own operation in the country. Even if they ultimately want to set up their own operations, these could serve as a transitional arrangement. Outsourcing to meet the AIFMD requirements will enable them to enjoy continued access to the EU without immediately needing to deploy staff abroad in what is likely to be an uncertain post-Brexit period.

1 <http://uk.reuters.com/article/us-britain-eu-banks-idUKKBN14W00A>

2 <https://www.esma.europa.eu/press-news/esma-news/esma-advises-extension-funds-passport-12-non-eu-countries>

WHEN DO YOU BELIEVE BREXIT WILL IMPACT YOUR COMPLIANCE ARRANGEMENTS?







**Author**

**Nick Bayley**

Managing Director  
Regulatory Consulting  
Duff & Phelps  
nick.bayley@duffandphelps.com

## Navigating the MiFID II Maze

The European Commission started work on the MiFID II Directive back in 2011; in mid-2014, the Level 1 legislation was finalised.<sup>1</sup> The Commission finished implementing the legislation in 2016, and ESMA has been churning out Level 3 guidance and Q&A across a variety of topics ever since.

With a deadline for implementation of January 2018, MiFID II represents a herculean achievement on the part of policymakers and regulators, the likes of which we are unlikely to see in financial services rulemaking for quite some time. Thank goodness, many of you will say.

At its heart, MiFID II has a handful of key themes: market structure, conflicts of interest, transparency, conduct of business, reporting to regulators and consistency across the EU. The sheer length and complexity of the MiFID II legislation is astounding. In addition to its size and scope, MiFID II will bring fundamental changes to many current market practices.

Unsurprisingly, a cottage industry of service providers has sprung up to offer solutions around MiFID II – in particular, a plethora of technology providers claim they can help firms handle the new requirements. Some of these firms are well-established names that have identified MiFID II as an opportunity to extend the scope of their existing services to meet clients' needs, while many are niche providers offering a single solution to a particular regulatory challenge.

Navigating the different providers and identifying cost-effective technology and system solutions without introducing over-complex or over-engineered processes is challenging. MiFID II represents an opportunity for many firms to take a more strategic approach to how they manage

their data, how they report to regulators and how they communicate with their clients. A short-term, piecemeal approach to dealing with MiFID II is likely to result in firms spending more time and effort further down the line and could entail missing some of the opportunities that the legislation presents.

In addition, there are commercial benefits to be found in the challenge of MiFID II. An example of this is in relation to best execution obligations. A firm that views best execution as an issue for compliance and simply a series of rules to be adhered to may be missing out on a strategic opportunity. The front office can derive clear benefits from having the right execution-quality tools, which enable traders to use real data to weigh the

<sup>1</sup> <https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir>

relative importance of execution factors – price, certainty, timeliness, etc. – which can add real commercial value.

The cost of MiFID II to the industry is significant and certainly exceeds the sub-euro 1 billion amount set out in the European Commission's original cost/benefit analysis. The mantra of firms should be that if they are going to spend money on MiFID II, which they will have to, then it must be spent wisely.





**Author**

**Rosemary Fanelli**

Managing Director and Chief Regulatory Affairs Strategist  
Compliance and Regulatory Consulting  
Duff & Phelps  
rosemary.fanelli@duffandphelps.com

## What to Expect from Trump

### Changes for investment firms or more of the same?

The president of the United States may not initiate legislation, but he enjoys the authority of the bully pulpit, as well as the presidential veto. With Republican majorities in both houses and little doubt about Donald Trump's willingness to call out Congress (and individual congressmen and congresswomen), one might expect an avalanche of changes.

However, despite promises to "dismantle" Dodd-Frank, changes are likely to be piecemeal, and the extent of reform (or otherwise) won't be clear for some time.

On the one hand, there may well be a modest relaxation in some filing and disclosure obligations for private equity funds. The Investment Advisers Modernisation Act, introduced during the last Congress, garnered broad bipartisan support, and Members of Congress have stated privately that they plan to reintroduce the bill into the current Congress.

On the other hand, some bills – even if enacted – might not result in much practical change for investment firms. The Financial CHOICE Act, part of

which would have removed entirely the obligation for private equity firms to register, faces an uncertain future.

For example, a newly reintroduced bill may not contain the private equity exemption provisions; the bulk of the CHOICE Act is focused on the Volcker Rule and easing regulations on community banks. For the President, passage of those provisions would probably be sufficient to make good on his promise to deregulate.

Furthermore, even if private equity firms are relieved of regulatory disclosure requirements, investors have unquestionably grown used to the level of information these firms have been required to provide. It is not likely large

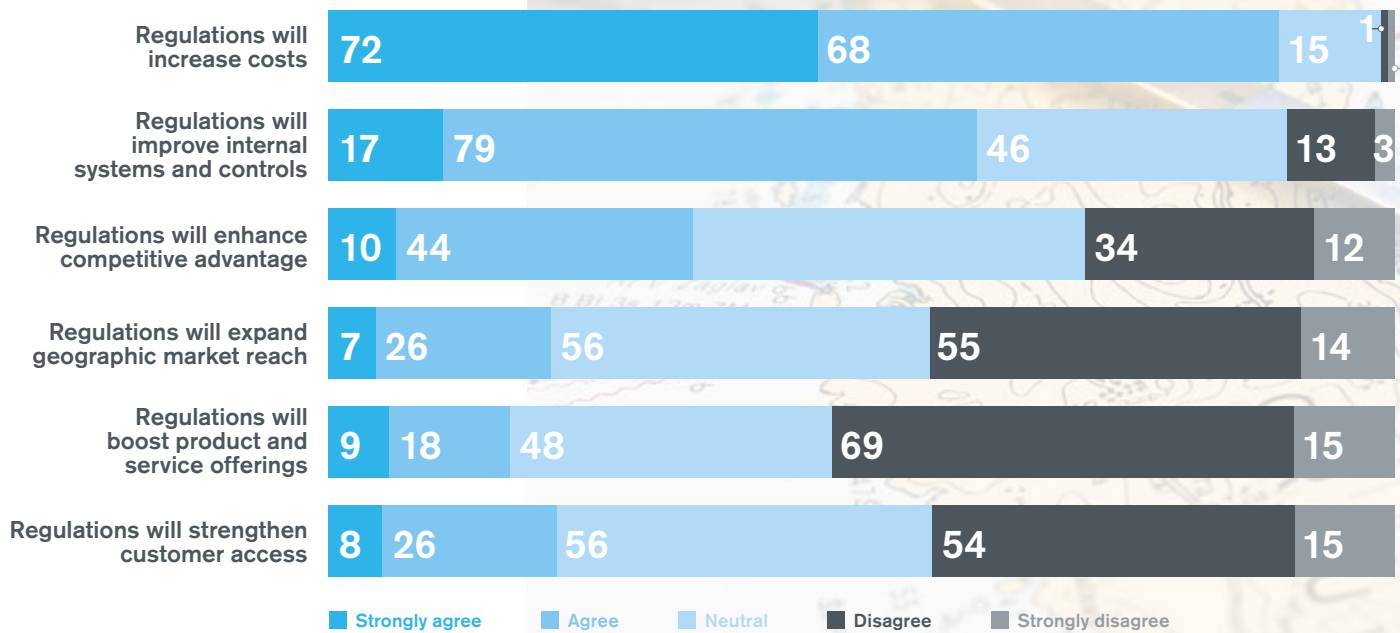
institutional investors will accept less information and fewer disclosures. Notwithstanding the President's bold attempts at deregulation, he cannot be expected to unscramble the eggs.

Additionally, it will be left to the SEC to define what is meant by "private equity firm", a definition that may include an assets threshold, buyout strategy or other limitation. At a minimum, we can expect these firms to be required to continue to make certain disclosures and be required to have certain compliance policies, by virtue of existing law, the CHOICE Act, investors or all of the above.

Finally, regulators have grown adept at expanding obligations through reinterpreting existing regulation.



IMPACT OF REGULATIONS ON YOUR FIRM IN 2017



The SEC, for example, has used the traditional fiduciary duty concept to bring a variety of cases over such diverse issues as business continuity, cybersecurity, and allocation of fees and expenses, without support from any specific rules whatsoever.

Indeed, ironically, sometimes the only way to restrain regulators is through more regulation, not less. One other area where Trump’s influence may be felt, for example, is by support of a bill to ban insider trading. This would give a clear, uniform basis to the prohibition and, crucially, define to whom it applies – removing ambiguity that, rather than weakening enforcement, has allowed the SEC and Justice Department to flex their muscle in the ambiguous grey zone.



**Author**

**Norm Champ**

Former Director, Division of Investment Management at the SEC  
Partner  
Kirkland & Ellis

## Draining the Swamp?

It was a political earthquake, but the impact of Donald Trump's surprise election victory will depend on where you look.

It's possible to both overstate and underestimate the changes Donald Trump could bring to U.S. financial regulation.

On one hand, America has a new president, but largely the same SEC. When it comes to the U.S. Treasury, the president appoints the top 340 people. Under the authorising legislation governing the SEC, he will appoint three commissioners – one of them chosen by the (Democratic) Senate Minority Leader Chuck Schumer. Two others, one Republican and one Democrat, remain in place.

With Mary Jo White's decision to step down early, Trump's appointments include the SEC chair. With that comes the power to set the agenda of what the commission will consider and vote on. It means, for instance, that those concerned about Senator Elizabeth Warren's proposals to force companies to disclose political contributions can probably rest easy.

Set against that, though, the other 4,000 staff at the SEC remain securely in place. They are as close as you will find to the definition of a permanent bureaucracy. Staffing at the 1,000-strong Office of Compliance Inspections and Examinations will remain essentially unchanged; likewise, at the Division of Enforcement, which, with about 1,400 people, is the single largest group in the commission.

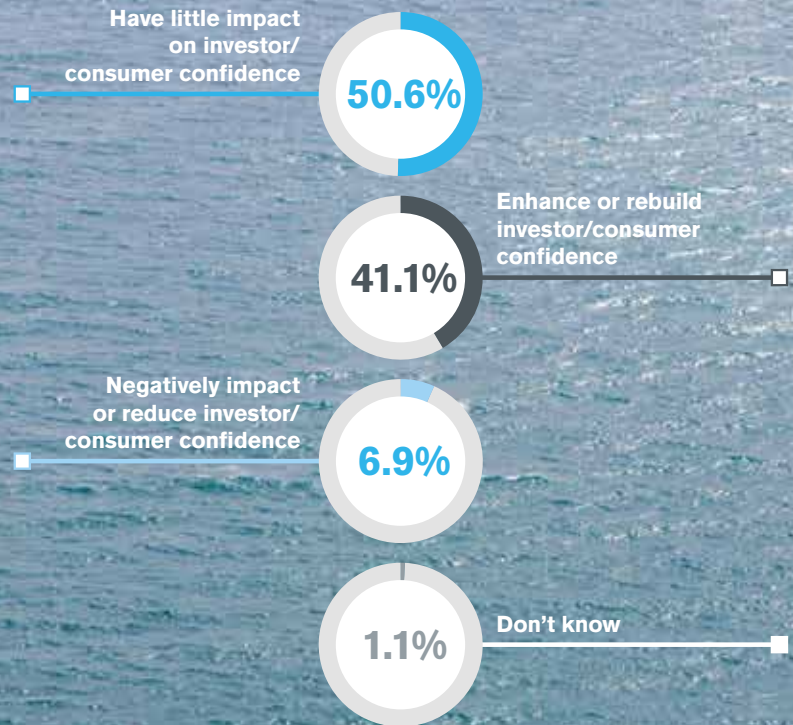
There may be some changes at the margins: for example, it will be interesting to see if the flurry of cases against private equity firms in the past couple of years continues, given that three out of the five commissioners must approve any case brought by the staff. Wholesale change in the approach to examination or enforcement is unlikely, however. It's going to be business as usual.

### **Changing the rules**

When it comes to rulemaking or perhaps rule removing, there is much greater scope for a new direction. Trump may not actually "dismantle" Dodd-Frank, but there is room for a considerable reduction in some of the more unnecessary regulations. Mutual fund board duties, massively expanded in recent years, are ripe for rationalisation. Private equity firms may not be freed from registration as investment advisors, but could see changes to accommodate them and reflect the fact that the regime is built for firms actively trading securities.

For broker-dealers, there may be opportunities to look again at the impact of the Volcker Rule on liquidity, particularly in the bond markets.

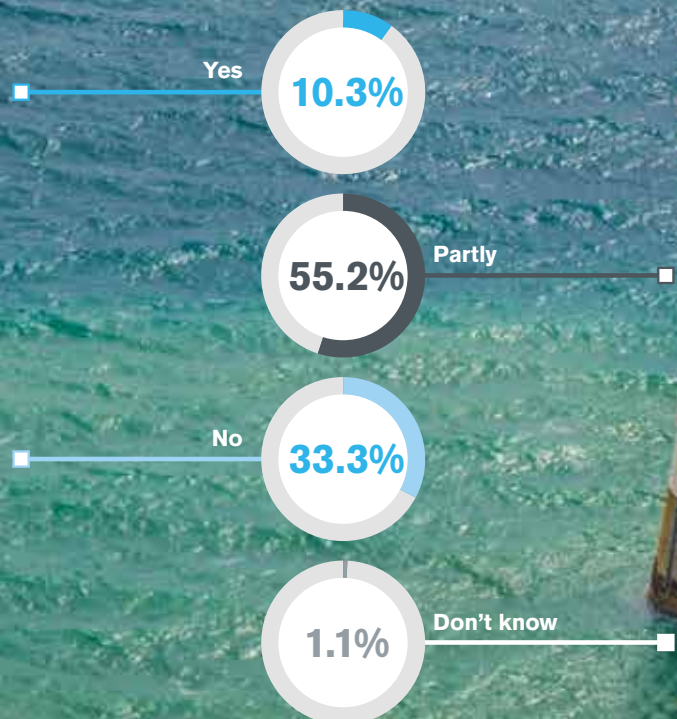
WHAT IMPACT DO YOU BELIEVE REGULATION IN THE FINANCIAL SERVICES INDUSTRY WILL HAVE ON INVESTOR/CONSUMER CONFIDENCE IN 2017?



Perhaps the biggest scope for changes is in corporate finance and addressing the decline in IPOs. The U.S. needs to examine the requirements in place that make going public unattractive to companies. From pay ratio disclosure rules<sup>1</sup> to reporting of resource extraction payments<sup>2</sup> and conflict minerals,<sup>3</sup> there is a long list of recently introduced regulation that risks eroding the U.S.'s position as a leading listings venue.

There are not that many industries where the U.S. continues to dominate, but its capital markets remain the envy of the world. As new financial centers continue to develop and emerge elsewhere in the world, the new administration should not take this for granted.

DO YOU BELIEVE THAT REGULATORY CHANGES OVER RECENT YEARS HAVE ADEQUATELY CREATED SAFEGUARDS TO PREVENT A FUTURE CRASH?



1 <https://www.sec.gov/news/pressrelease/2015-160.html>  
 2 <https://www.sec.gov/news/pressrelease/2016-132.html>  
 3 <https://www.sec.gov/News/Article/Detail/Article/1365171562058>





**Author**

**David Larsen**

Managing Director  
Alternative Asset Advisory  
Duff & Phelps  
david.larsen@duffandphelps.com

## No Right Answer

Valuations of illiquid assets continue to trouble regulators. Half a decade on from Dodd-Frank in the U.S. and the EU's Alternative Investment Fund Managers Directive (AIFMD), regulators – and the fund managers they oversee – are still finding their way.

The problem is there are no easy answers. Regulators and funds must balance the need for independent valuations against the fact that fund managers are usually the best placed to provide accurate appraisals of hard-to-value assets.

Under regulations like the Investment Company Act of 1940 and EU AIFMD, fund managers have a clear responsibility to give fair value estimates. And regulators are willing to give this obligation teeth. The U.S. has seen a number of enforcement actions and even litigation<sup>1</sup> focused on valuations in the past year.<sup>2</sup>

The SEC is looking at all types of misconduct by hedge fund managers. "Valuation is one of the core issues,"<sup>3</sup> its enforcement, director Andrew Ceresney, has said.

Elsewhere, Hong Kong's SFC issued a circular in 2015 to provide further guidance to managers on valuations.<sup>4</sup> Informally, all regulators have also been attempting to develop in-house expertise in valuation.

As such, managers should expect increased scrutiny – and, most likely, an increased level of enforcement action both outside and inside the U.S. – going forward.

**Buyer beware**

Nevertheless, while regulators are keen to insist on that respect for the principles of fair valuation, many of the mechanics remain outside their purview.

As a result, the responsibility for ensuring managers provide good fair-value estimates must still rest largely with investors – and particularly institutional

investors who can reasonably be expected to carry out this level of due diligence.

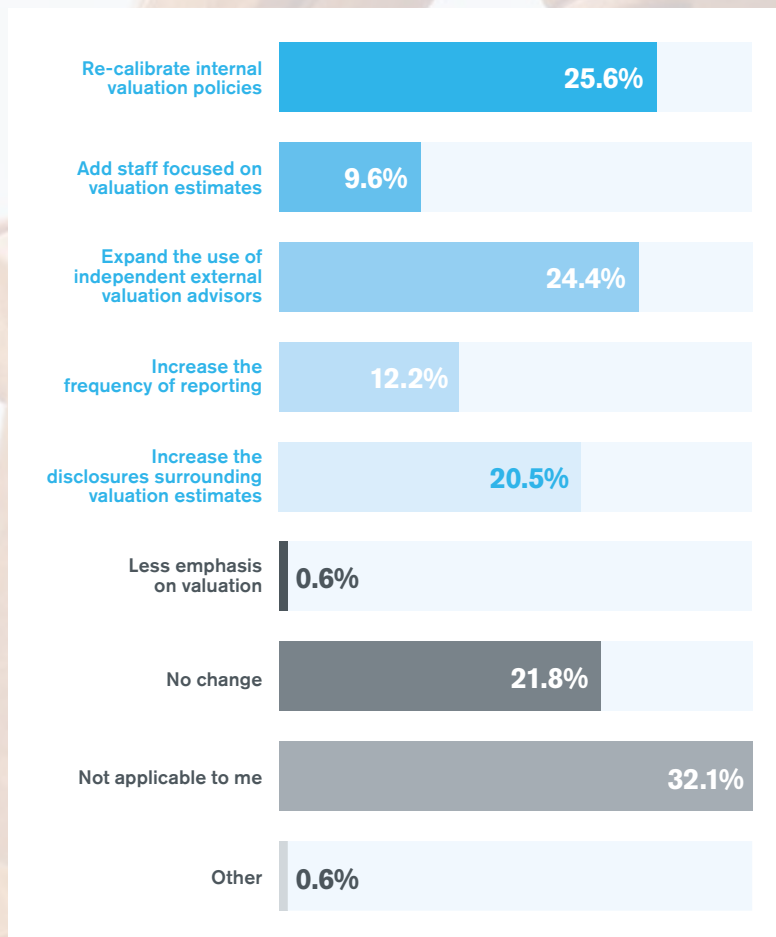
There are two related dangers. The first is that independence is blindly applied. An independent process is vital; but independent valuation without input from the deal team, which has the greatest insight on the assets, is likely to undermine the object of the exercise.

The second is an overreliance on audit and appraisal. Both are valuable tools, but hearing the words alone should not be enough. Investors must, as regulators increasingly will, consider the expertise and process involved, and whether this genuinely contributes to a robust, rigorous valuation.

There are, as said, no easy answers. While regulators and funds continue to wrestle with the issues, though, investors cannot afford to stop asking questions.

1 <https://www.sec.gov/litigation/admin/2016/33-10111.pdf>  
2 See for example <https://www.sec.gov/news/pressrelease/2016-11.html>  
3 <http://www.wsj.com/articles/hedge-funds-treatment-of-investors-gets-new-scrutiny-1462808155>  
4 <http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=15EC41>

IN WHICH OF THE FOLLOWING WAYS DO YOU EXPECT TO ENHANCE THE RIGOR SURROUNDING YOUR VALUATION PROCESSES IN 2017?



# CYBERSECURITY







请勿攀爬  
DO NOT CLIMB

**Author****Adam Menkes**

Director

Credit Suisse

# No Simple Exercise

## Risk, not rules, must determine firms' cybersecurity requirements.

The SEC's decision to issue guidance rather than specific requirements around cybersecurity has led to some uncertainty among registered investment advisors (RIAs) over how to implement certain aspects of their cybersecurity programs.

Without a clear statement of their expected obligations, many RIAs report that it has been difficult to determine if they have done enough to satisfy the SEC and investors alike. That said, the majority of firms have formed a strong base and continue to focus on improvements, as the threat landscape continues to evolve.

Over time, the SEC and other regulators have issued substantial guidance on their key areas of focus, and RIAs have realized that taking action based on that guidance rather than waiting for specified regulations is the right approach. In April 2015,<sup>1</sup> the SEC suggested investment companies and advisors “may wish to consider”, among other things, risk assessments, a cybersecurity strategy, and written policies and procedures as well as training.

The Office of Compliance Inspections and Examinations (OCIE) initiative in September of that year outlined broker-dealers' and investment advisors' controls.<sup>2</sup>

In addition to the OCIE,<sup>3</sup> regulatory bodies such as Financial Industry Regulatory Authority (FINRA)<sup>4</sup> have provided additional guidelines for managers to look to. While following these other requirements may hold managers to a higher standard than is outlined by the OCIE, there is little indication to date to suggest that the SEC's expectations are lower. Historically, the SEC and FINRA have been quick with enforcement action where their guidelines have been egregiously ignored. The number of cases brought by these two regulators on the basis of cybersecurity failings (at least in part) is already in the double digits.

**To each their own**

Set in this context, the SEC's lack of specificity gives it the flexibility to evaluate each RIA's adherence to the guidelines independently. The areas where the regulator will spend its time are increasingly clear; encryption, data retention limits, risk assessments, information security policies, documentation, incident response plans and workforce training are all fair game. It seems that there is to be, for now, no definitive or official list of requirements that RIAs can simply check off to claim compliance. In firms where the SEC sees the higher potential risk, it has left itself room to demand greater measures to protect against cyber threats, and lesser measures for threats that pose a lower risk.

<sup>1</sup> <https://www.sec.gov/investment/im-guidance-2016-04.pdf>

<sup>2</sup> <https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf>

<sup>3</sup> <https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf>

<sup>4</sup> <http://www.finra.org/newsroom/2015/finra-issues-report-cybersecurity-practices-cybersecurity-investor-alert>

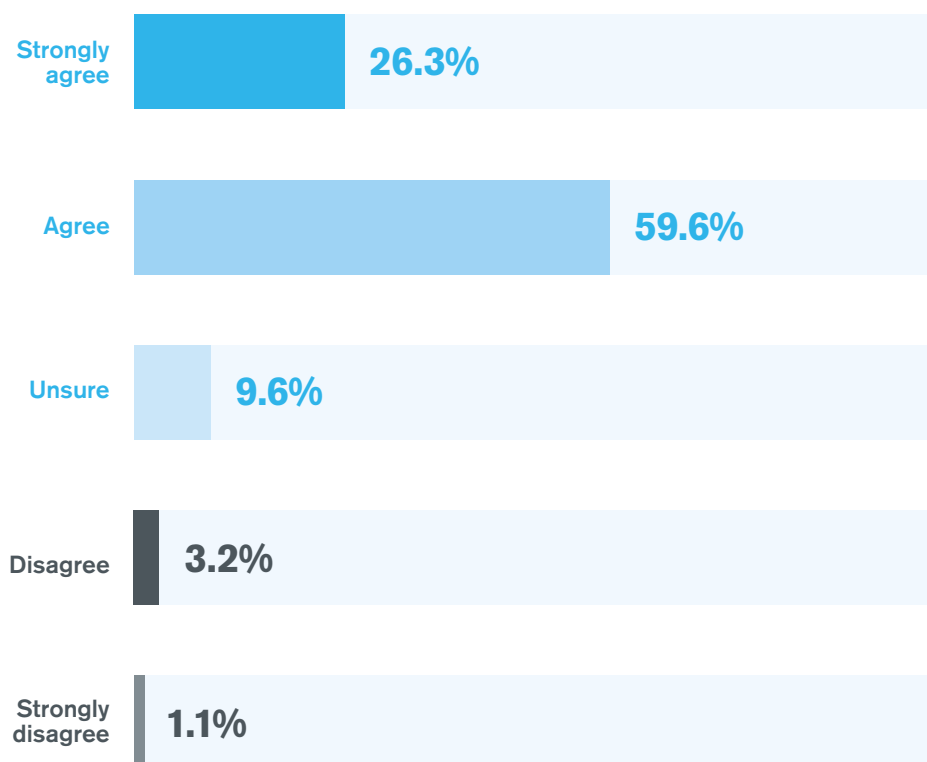
**WHERE DO YOU EXPECT REGULATORS TO FOCUS IN 2017?**

| Focus Area        |                  |                                    |                        |                               |                        |                                |                |                            |                                |   |                      |  |                                      |                                 |           |            |                |
|-------------------|------------------|------------------------------------|------------------------|-------------------------------|------------------------|--------------------------------|----------------|----------------------------|--------------------------------|---|----------------------|--|--------------------------------------|---------------------------------|-----------|------------|----------------|
| Answer Options    | Accounting fraud | AML/KYC and financial crime issues | Asset misappropriation | Benchmark and FX manipulation | Bribery and corruption | Client suitability/mis-selling | Cyber-security | Fee and expense allocation | Firmwide culture of compliance | High-frequency, dark pools, algo and electronic trading | Liquidity management | Marketing practices to investors/customers | Misstating/misreporting asset values | Proper disclosure for investors | Valuation | Don't know | Response Count |
| <b>Priority 1</b> | 1                | 34                                 | 2                      | 2                             | 5                      | 7                              | 48             | 16                         | 9                              | 2   | 8                    | 6  | 0                                    | 10                              | 4         | 3          | <b>157</b>     |
| <b>Priority 2</b> | 2                | 17                                 | 0                      | 2                             | 4                      | 11                             | 35             | 19                         | 14                             | 11  | 7                    | 14   | 3                                    | 9                               | 6         | 2          | <b>156</b>     |
| <b>Priority 3</b> | 5                | 11                                 | 3                      | 4                             | 12                     | 7                              | 21             | 7                          | 22                             | 7   | 5                    | 17   | 3                                    | 18                              | 6         | 4          | <b>152</b>     |

This is not necessarily a bad thing. While RIAs may have less certainty about cyber compliance, they also have an opportunity to look at cybersecurity holistically and pragmatically. This should prompt them to consider not just the regulatory requirements, but also their own cybersecurity risks.

The SEC is rightly focused on investor protection and market integrity. Firms' intellectual property or client lists (from a competitive, rather than privacy, standpoint) are not really its concern. Meeting the SEC standards will not necessarily protect a firm's algorithms, nor retain its customers when a trader leaves. Cybersecurity must go further than minimal compliance satisfaction. To an extent, the SEC's flexibility means that it will continue to determine whether RIAs' cybersecurity controls are adequate on a case-by-case basis, and RIAs likely should be taking the same approach.

**GIVEN THE MAGNITUDE OF RECENT CYBER BREACHES, OUR COMPANY PLANS TO FOCUS MORE RESOURCES AND TIME ON CYBERSECURITY.**







**Author**

**Sharon Cohen Levin**

Partner

WilmerHale

# The Convergence of AML and Cybersecurity

Cyber breaches have become an unwelcome staple of our era, from the report that 1 billion Yahoo accounts were hacked to the massive theft of data from the Office of Personnel Management and ongoing threats and breaches at financial institutions, hospitals, technology companies and military contractors.

Financial institutions are particularly attractive targets for cyber attacks, given their massive store of sensitive data accessible on electronic information systems. Cybersecurity has thus emerged as a high priority for financial regulators and the institutions they supervise. During the past year, we have seen the convergence of cybersecurity with another pressing topic in the financial industry: Anti Money Laundering (AML). We expect this convergence to accelerate in 2017.

Financial institutions have traditionally handled cybersecurity and AML compliance separately, with cybersecurity responsible for protecting information systems while AML compliance monitors transactions for indicia of money

laundering and terrorist financing. The two groups typically operate with separate personnel and reporting lines. While there are practical reasons for financial institutions to maintain separate cybersecurity and AML units, U.S. regulators have come to expect that financial institutions will take a holistic view of cyber threats and incorporate information about cyber-events and cyber-enabled crimes in Suspicious Activity Reports (SARs) filed pursuant to their Bank Secrecy Act obligations.

In October 2016, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued an advisory (the "Advisory") addressing a financial institution's suspicious activity reporting

obligations related to cybercrime.<sup>1</sup> The Advisory states that even if a cyber-event does not result in a "transaction," a financial institution must still file an SAR if it "knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate or effect a transaction or series of transactions."<sup>2</sup> Under this broad mandate, financial institutions should consider the possibility of filing an SAR after any cyber-event, even if the primary objective does not appear to be the theft of funds. To determine when a cyber-event requires the filing of an SAR, financial institutions must take into account the nature of the event and the information and systems it targeted. In the Advisory and its accompanying set of frequently asked

<sup>1</sup> FinCEN, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime, FIN-2016-A005 (Oct. 25, 2016), available at [https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508\\_2.pdf](https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf).

<sup>2</sup> Id. at 4.



questions, FinCEN provides detailed guidance on the reporting of cyber-events, cyber-related crimes and cyber-related information.

In the Advisory, FinCEN encourages financial institution cybersecurity units to share information with their AML compliance counterparts. According to FinCEN, such collaboration would “help financial institutions conduct a more comprehensive threat assessment and develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime.”<sup>3</sup> FinCEN also recommends that financial institutions share cyber-related information among themselves for the purpose of identifying and, where appropriate, reporting potential money laundering or terrorist activities.<sup>4</sup>

In a previous advisory, issued in September 2016, FinCEN warned financial institutions about e-mail compromise fraud schemes in which criminals deceive financial institutions and their customers into transferring funds.<sup>5</sup>

The September advisory noted that this type of cyber-enabled financial crime may trigger a financial institution’s suspicious activity reporting requirements under applicable AML regulations. In sum, FinCEN, through these advisories, has set forth the clear expectation that financial institutions will file SARs on cyber-related events and cyber-enabled crime. Failure to do so could result in regulatory scrutiny and possible civil or criminal penalties.

The FinCEN guidance is part of a broader governmental effort to detect and prevent cybercrime. In October 2016, the federal banking regulators issued a joint advance notice of proposed rulemaking concerning cybersecurity regulations and efforts to improve the safety and soundness of the U.S. financial system.<sup>6</sup> State regulatory bodies are also focused on cybercrime and AML, proposing new requirements on the entities they regulate. For example, the New York Department of Financial Services (DFS) has advanced new rules that prescribe minimum criteria for AML and cybersecurity programs and require financial institutions to certify compliance with the standards.

In June 2016, DFS issued a final rule prescribing minimum standards for AML transaction monitoring and filtering programs.<sup>7</sup> The rule, which requires the board or a senior officer of each covered financial institution to certify compliance, went into effect in January 2017. In September 2016, DFS proposed a similar rule with respect to cybersecurity.<sup>8</sup> If issued, the rule would prescribe minimum standards for cybersecurity programs and require the board or a senior officer of each covered financial institution to certify compliance.

Given the regulatory focus on cybersecurity and AML issues, financial institutions need to increase collaboration and communication between their AML compliance and cybersecurity personnel. In particular, financial institutions should ensure that their cybersecurity and AML compliance personnel understand 1) when a cyber-event should be escalated to the attention of AML compliance and 2) the cybersecurity and AML compliance information needed to satisfy emerging reporting requirements from regulators.

<sup>3</sup> Id. at 7.

<sup>4</sup> To encourage such sharing, Section 314(b) of the USA PATRIOT Act extends a safe harbour from liability to financial institutions that notify FinCEN and satisfy certain other requirements in connection with the information sharing.

<sup>5</sup> FinCEN, Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes, FIN-2016-A003 (Sept. 6, 2016), available at <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003>.

<sup>6</sup> Joint Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk Management Standards (Oct. 19, 2016), available at <https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf>.

<sup>7</sup> New York Dept. of Financial Services, Final Rule, Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications (June 30, 2016), available at <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf>.

<sup>8</sup> New York Dept. of Financial Services, Proposed Rule, Cybersecurity Requirements for Financial Services Companies (Sept. 13, 2016), available at <http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf>.

**Author****Jason Elmer**

Managing Director  
 Compliance and Regulatory Consulting  
 Duff & Phelps  
[jason.elmer@duffphelps.com](mailto:jason.elmer@duffphelps.com)

# Preparing for and Responding Effectively to Cyber Attacks

Cybersecurity is the biggest risk facing the financial system, according to outgoing SEC Chair Mary Jo White, and as such firms can expect it to increasingly be a regulatory focus going forward. As she put it, “We can’t do enough in this sector.”<sup>1</sup>

It’s not just the rhetoric that has reached new heights; in June, the SEC appointed IT security expert Christopher Hetner as a senior adviser “coordinating efforts across the agency to address cybersecurity policy.”<sup>2</sup> In addition, cybersecurity compliance was among its examination priorities in 2016 and is likely to carry on into 2017.

So far, the SEC hasn’t mandated specific standards for firms. Nevertheless, the agency has already taken enforcement action in cases where it has deemed that inadequate cybersecurity policies and procedures fall foul of the federal “Safeguard Rule” – Rule 30(a) of Regulation S-P under the Securities Act of 1933.

“Firms must adopt written policies to protect their clients’ private information, and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs,” it noted.<sup>3</sup>

**A worldwide focus**

The SEC is far from alone among U.S. regulators in focusing on cyber issues. In March, the National Futures Association’s (NFA) Cybersecurity Interpretive Notice, approved by the Commodity Futures Trading Commission, came into effect. Regulated businesses must have an information systems security program appropriate to their circumstances, even if there is flexibility in determining what that is. In May, FINRA too published

a checklist for small firms creating a cybersecurity program.<sup>4</sup>

Financial regulators elsewhere are also increasingly taking the mantle from – or perhaps more often working with<sup>5</sup> – the data protection bodies that have driven enforcement of cybersecurity standards to date.

Laying out the UK regulator’s approach in September, the FCA’s director of specialist supervision said it intends to broaden its existing focus on the largest financial services providers to include smaller firms.<sup>6</sup> In a circular in October, Hong Kong’s FSC, meanwhile, identified cybersecurity management as a priority for its supervision, noting the number of hacking incidents it had seen in the past year.

1 <http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4>

2 <https://www.sec.gov/news/pressrelease/2016-103.html>

3 <https://www.sec.gov/news/pressrelease/2015-202.html>

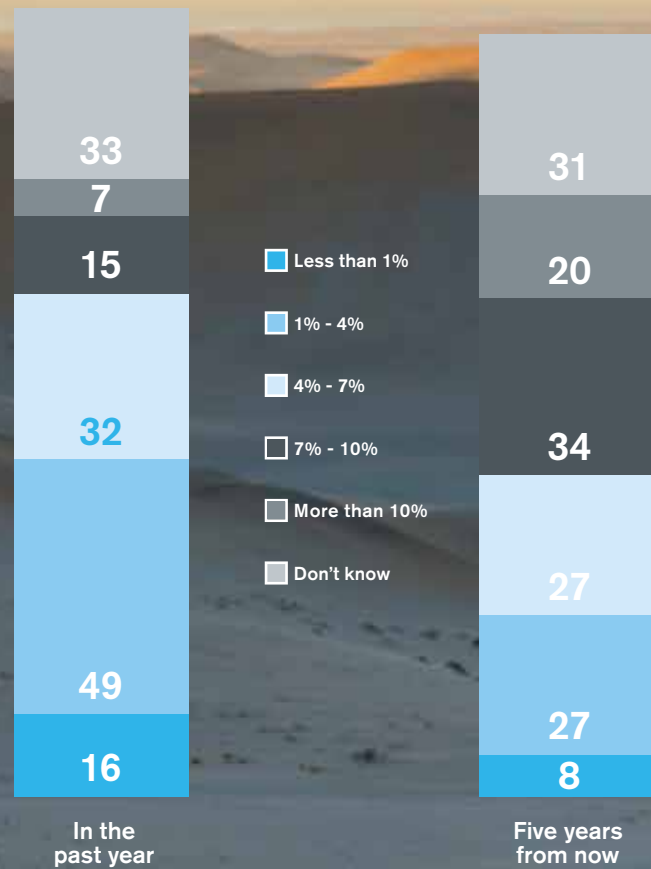
4 <http://www.finra.org/industry/small-firm-cybersecurity-checklist>

5 <https://www.fca.org.uk/publication/mou/mou-fca-ico.pdf>

6 <https://www.fca.org.uk/news/speeches/our-approach-cyber-security-financial-services-firms>



AS A PERCENTAGE OF ANNUAL REVENUE, HOW MUCH DO YOU BELIEVE YOUR COMPANY SPENT OR WILL SPEND ON COMPLIANCE?

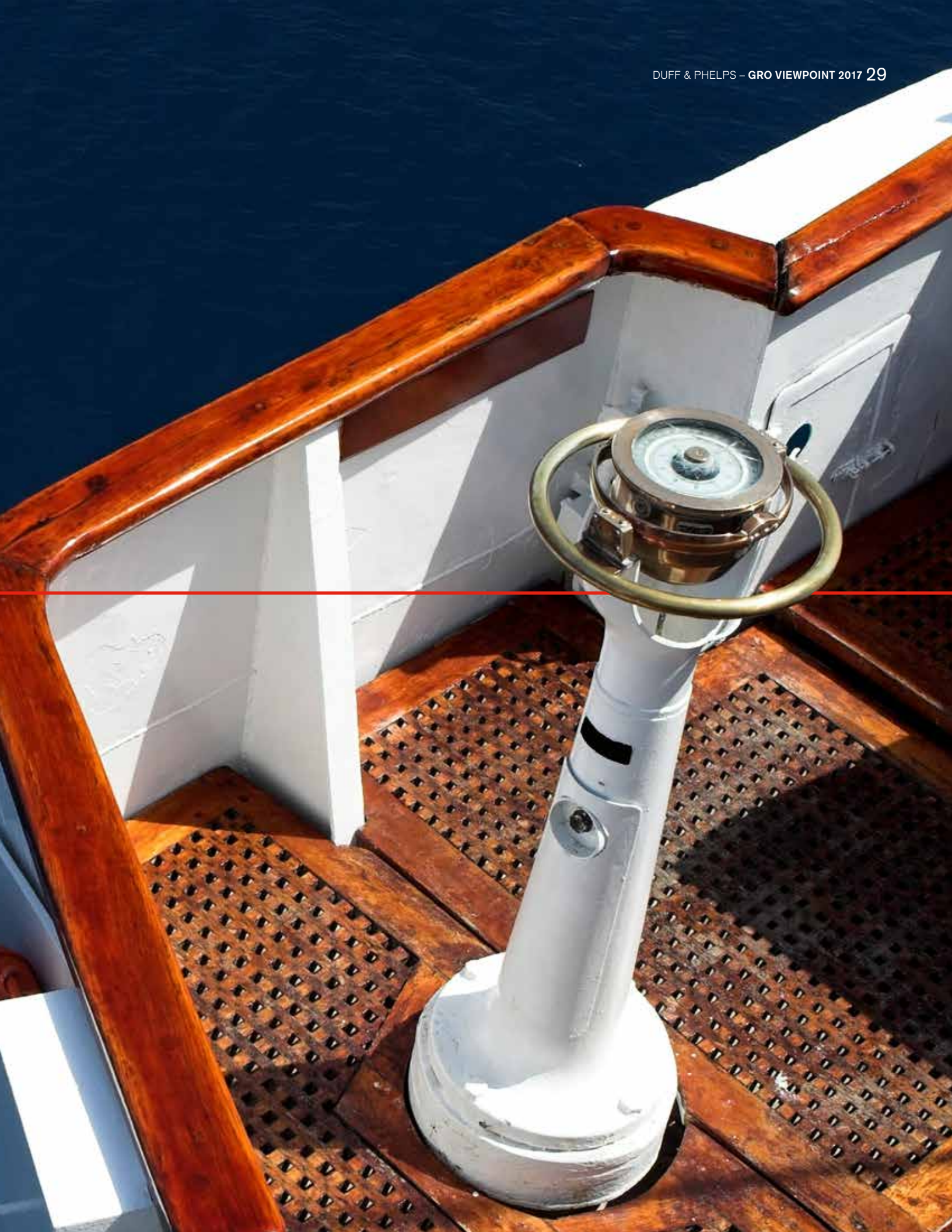


“While these hacking incidents are still under police investigation, there are indications that brokers and their clients may be able to do more to better protect online trading accounts,” it said.

Whether this interest from regulators will bring about new rules remains to be seen, but increasing attention – and enforcement action – under existing requirements seems likely. Even without this, though, it is worth noting that increasing and high-profile attacks are prompting investors to ask many of the same questions about cybersecurity as regulators are posing. Commercial forces, as well as regulatory pressures, are ultimately likely to prove key in improving standards.

# INDIVIDUAL ACCOUNTABILITY







**Author****Monique Melis**

Managing Director and Global Head of Regulatory Consulting  
 Duff & Phelps  
 monique.melis@duffandphelps.com

# Having an Impact

## Senior manager regimes in the UK and elsewhere

Individual accountability is finally becoming a reality. After years of talk, 2016 was the year that it began to bite in the banks. For many financial services firms, it's a sign of things to come.

The UK's Senior Management and Certification Regime was introduced last March for banks, building societies and credit unions. It has undoubtedly made certain roles within these institutions less appealing as they carry a greater degree of personal risk. Individuals will now think twice about taking on roles that may ultimately cost their career. This will undoubtedly extend to the compliance officer, MLRO and head of risk. Those already in these roles will be harder to retain and will be worried if they feel that they don't have the support they need to do the job. We have arguably already seen examples of this.

There are many other well paid roles within regulated institutions that may seem more appealing and don't fall under regulatory scrutiny. This may have a knock on effect on certain roles, simply because not enough skilled staff want to take on the personal regulatory risk. The question

then becomes; are these regulated firms willing to increase compensation enough to cover the risk? We have not yet seen this shift but clearly it must be a consequence. Ultimately, then, the regime may give rise to unintended consequences resulting in real difficulty to fill such posts – at the risk to the institution.

**Sticking with what works**

Yet the Financial Conduct Authority (FCA) is likely to stick with its agenda – and others will soon feel its effects. Next year, in the UK, the regime will be extended to investment firms and asset managers. In Hong Kong, the SFC has introduced its new Managers-in-Charge regime through a circular<sup>1</sup> issued in December along with a list of frequently asked questions.<sup>2</sup> The SEC, meanwhile, continues its enforcement action against 'gatekeepers' that fail in their duties to prevent financial crime.<sup>3</sup>

The reason is simple: with these regimes, personal accountability is having an impact. The threat of personal sanctions is ensuring compliance functions put their duties before other considerations. Where managers fail to support them, they themselves may face penalties.

Even if senior managers are reluctant to pay compliance functions more, the regime should eventually lead them to budget differently for compliance: counting not just compliance costs, but the costs of hiring a replacement compliance officer or interim staff; for regulatory penalties and remediation in cases of failure; and for their own personal liability potentially if things go wrong.

In short, this new regime may be a game-changer. Almost a decade after the financial crisis, cultural change in financial services is finally starting to happen.

<sup>1</sup> [www.sfc.hk/edistributionWeb/gateway/EN/circular/openFile?refNo=16EC68](http://www.sfc.hk/edistributionWeb/gateway/EN/circular/openFile?refNo=16EC68)

<sup>2</sup> <http://www.sfc.hk/web/EN/faqs/intermediaries/licensing/manager-in-charge-regime.html#26>

<sup>3</sup> <https://www.sec.gov/news/pressrelease/2016-120.html>





**Authors**

**Tim Mak**

Partner

Freshfields Bruckhaus Deringer



**Wings Turkington**

Senior Knowledge Lawyer

Freshfields Bruckhaus Deringer

## The SFC's new "Managers-in-Charge" Regime: it's getting tougher at the top

Regulators in key markets around the world have increasingly looked for more effective ways to hold senior managers of financial institutions accountable for wrongdoing within their institutions, driven by the belief that overall corporate behaviour can be improved through increased personal responsibility.

In Hong Kong, after concerted reminders from the Securities and Futures Commission (SFC) and other regulators that senior management of financial institutions must foster the "right corporate culture," and that individuals will be held accountable for misconduct, the SFC recently published the Circular "Regarding Measures for Augmenting the Accountability of Senior Management." That Circular and its accompanying FAQs aim to reinforce that message and give additional guidance.

The guidance builds on expectations of senior management in the SFC's Code of Conduct, and confirms that the SFC regards a Licensed Corporation's (LC) Board of Directors, its Responsible Officers (ROs) and individuals designated by that LC as "Managers-in-Charge" (MICs) as "senior management."

Who should be designated an MIC? LCs must appoint at least one MIC, each of whom should report directly to the Board or CEO, for each of the following eight "Core Functions": overall management oversight (those who direct/oversee operations daily, e.g., CEO), key business line (those who direct/oversee a regulated activity, e.g., head of that business line), operational control and review (e.g., COO), risk management, finance and accounting, information technology, compliance, and anti-money laundering. Existing LCs are expected to give the SFC between 18 April 2017 and 17 July 2017 MIC information and new organisational charts which show a clear management and governance structure and individual reporting lines.

What does all of this mean for an LC in practice? As a start, it will necessitate

a fresh look by its Board and senior management of its management, organisational, reporting and responsibility structures, to identify which individuals have responsibility for what areas, to whom they have responsibility and why, so that those structures are clear and can be documented, and at least one MIC for each Core Function can be identified. It will then require buy-in from those individuals before the SFC can be notified of their MIC designation ahead of the proposed 17 July 2017 deadline.

What challenges might arise along the way? Some individuals who should be designated MICs will be familiar with being regulated in Hong Kong (most key business line MICs will already be ROs because of their responsibilities). But some may not be so used to being under SFC scrutiny and, potentially,



exposure. For example, heads of risk management, finance and accounting, IT, and compliance, who do not typically hold SFC licences, may need particular help in understanding what being an MIC means for them. This also applies to any individuals located outside Hong Kong who have the SFC's expected attributes of an MIC (essentially, someone who has significant influence and decision-making power over a Core Function). Accordingly, it will be particularly important for those categories of MIC to be specifically educated about the MIC regime, their responsibilities within that regime and what it means for them to be identified as an MIC, so that their early buy-in can (hopefully) be obtained.

As for the standards of conduct expected of MICs, SFC expectations ought to be familiar territory for those who are already ROs, but may well not be for those who do not hold an SFC licence. In this regard, neither the Circular nor its accompanying FAQs appear to be particularly clear about the applicable benchmarks. Time, and the SFC's first disciplinary actions against unlicensed MICs, will tell how the SFC might look to enforce its MIC expectations in practice. But one thing is clear: it's getting increasingly tough at the top, and not just at the very top.





**Author**

**Nick Inman**

Managing Director  
Compliance and Regulatory Consulting  
Duff & Phelps  
nick.inman@duffandphelps.com

# The “Manager-In-Charge” Regime and Individual Accountability

As the SFC enhances accountability for senior managers of licensed corporations, this responsibility should be balanced with greater individual autonomy and authority.

There's a new sheriff in town, and he's keen to wrap up many of the matters that have been outstanding or going through due process for what is now considered an unacceptable length of time. The primary objective may be to focus on the bigger issues, but the short-term impact is an escalation in the number of issues addressed across the severity spectrum.

The timing is interesting, as also coming in on the next stagecoach, albeit being driven by licensing rather than enforcement, is the “Manager-in-Charge” (MIC) regime. Manager-in-Charge is a new category of senior management of a Licensed Corporation defined by the SFC, on top of directors and Responsible Officers (ROs). Licensed Corporations in Hong Kong will be required to nominate a number of senior individuals within their organisations as being the go-to people where there are difficult questions to be answered in regard to their chosen specialist subjects.

This presents major challenges for organisations of all sizes, not least of which is the fact that the time frame in which these individuals are to be identified and nominated is very tight.

There are complexities to address, in some cases job descriptions to be written, reporting lines to be formalised and even formal boards to be established. But perhaps more important for affected firms to address are those boundaries and grey areas where responsibility actually does become more difficult to define. Whilst it may be relatively clear who a Responsible Officer is for a business line, it may be less clear where ultimate responsibility for anti-money laundering or even risk lies. The result for a small firm may be that the SFC is none the wiser, as it will receive a form denoting that the two or three existing ROs are also holding all the MIC roles.

**Great responsibility should come with great(er) power**

The SFC has been at pains to point out that the MIC regime brings with it no new powers or laws. Be that as it may, it may represent a paradigm change for those individuals who now see their names in lights for the first time. Individual accountability or the lack thereof has been an undeniable global problem. But the potential conflict that these regimes introduce has to be managed. For individuals to accept that they are personally accountable, they need to be given more autonomy and authority. They need to be given budget for specialist projects to provide assurance that their area are operating as expected. Investment is required, both at the initial stage and thereafter, in management reporting mechanisms and ongoing validation. HR policies and procedures need to ensure formally assigned MICs are fully aware of their regulatory obligations, not to mention cross-border issues.

The interests of the individual may well diverge from those of the entity. What is beyond doubt is that individuals will be seeking some guidance from the SFC as to the yardsticks with which they will be measured. What the SFC will consider to be sufficient in discharging responsibility, or rather what might be construed as neglect, especially with the benefit of hindsight as is frequently the case, will

cause some consternation – and possibly some amendments to insurance policies (if this is allowed).

Given that the powers have always existed under the SFC to take “persons involved in the management of the business of an LC” to task, one might be forgiven for wondering whether the new regime will have any impact. The warning shot that it

represents, however, suggests that those designated as MICs would be foolish not to take it seriously and that we should all watch this space keenly.







**Author**

**Polly Greenberg**

Managing Director

Disputes and Investigations

Duff & Phelps

[polly.greenberg@duffandphelps.com](mailto:polly.greenberg@duffandphelps.com)

## U.S. Perspective on Enforcement Culture/Individual Accountability

For years U.S. regulators and prosecutors have been increasing the pace of financial crime-related actions brought against corporations. In past years this did not mean a similar increase in actions against individuals, though this is changing, since U.S. authorities have recently instituted several policies aimed at holding individuals accountable for acts committed on behalf of a corporate entity.

Many factors can make it difficult to prosecute individuals involved in corporate misbehaviour: disparate acts that together amount to misconduct can be committed by multiple people in an organisation, statutes of limitations (often waived by cooperating corporations but not by individuals) can run, and admissible evidence from overseas can be impossible to obtain. The new policies attempt to address those impediments.


In September 2015, the Department of Justice (DOJ) issued the Yates Memorandum, the basic premise of which is that corporations will not get credit for cooperating with the government unless they identify, provide evidence against and hold accountable culpable individuals in a timely manner. Further, when a corporation is charged

without accompanying charges against individuals, the investigation cannot be closed without a written, though not necessarily public, explanation as to why. These requirements demand enhanced prosecutorial focus on individuals. The Yates Memo also mandates more and earlier communication and cooperation between the DOJ's civil and criminal divisions. This may lead to more civil actions against individuals. Civil cases have a lower burden of proof, generally require a lesser showing of intent than do criminal charges and can sometimes be brought when there is insufficient evidence to support a criminal charge.

More recently, the DOJ announced the Foreign Corrupt Practices Act (FCPA) Pilot Program aimed at encouraging corporations to self-report issues and

remediation plans in connection with FCPA compliance. The Pilot Program confirms, in the FCPA context, that corporations will receive more lenient treatment if they cooperate with government investigations but, again, only if they also provide relevant evidence (where it exists) against individuals. To receive full credit, companies must exhibit good corporate citizenship. The government will evaluate their cultures of compliance by assessing resources devoted to compliance; employees' ability to understand and identify risky transactions; independence and reporting structure; compensation, promotion and disciplinary action; and effectiveness of the company risk assessment and audit program.

In June 2016, the New York State Department of Financial Services

A close-up photograph of a car's front end, focusing on the chrome grille and headlight area. The grille features a prominent circular emblem with a dark center and a chrome ring. The chrome is highly reflective, showing highlights and shadows. The background is a soft, out-of-focus blue sky.

(DFS) issued Rule 504. It lists specific expectations regarding transaction monitoring and filtering requirements that DFS-regulated financial institutions must employ in support of their anti-money laundering and Office of Foreign Assets Control sanctions programs. The original proposal required that a chief compliance officer or functional equivalent certify yearly that the institution has an effective compliance program, and it stated that inaccurate certifications could form the basis of criminal charges. While the final rule no longer references criminal charges, it states that it is not intended to “limit the Superintendent’s authority under any applicable laws.” Notably, DFS has demonstrated that it will hold individual compliance officers

accountable. For example, in recent years, DFS’s settlements of enforcement actions against financial institutions have sometimes required the termination of named employees not the subject of individual actions.

In sum, these policies demonstrate a government focus on individuals. They also reveal that regulators and prosecutors are looking closely at compliance cultures and existing programs in assessing corporate and individual culpability. Corporations must now provide evidence against individuals in a timely manner and hold senior employees explicitly accountable for the programs they manage.

**For more information please visit:**

**[www.duffandphelps.com](http://www.duffandphelps.com)**



# A POWERFUL PARTNERSHIP FOR A WORLD OF REGULATION.

**Kinetic Partners is now Duff & Phelps.**

Celebrating one year of offering leading compliance and regulatory guidance as Duff & Phelps. The same local experts, now working with you in a stronger, truly global network.

**Learn more at [duffandphelps.com](http://duffandphelps.com)**

DUFF & PHELPS

## **About Duff & Phelps**

Duff & Phelps is the premier global valuation and corporate finance advisor with expertise in complex valuation, disputes and investigations, legal management consulting, M&A, real estate, restructuring, and compliance and regulatory consulting. The firm's more than 2,000 employees serve a diverse range of clients from offices around the world. For more information, visit [www.duffandphelps.com](http://www.duffandphelps.com).

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory and capital raising services in the United Kingdom and across Europe are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorised and regulated by the Financial Conduct Authority. In Germany M&A advisory and capital raising services are also provided by Duff & Phelps GmbH, which is a Tied Agent of DPSL. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.

This material is offered for educational purposes with the understanding that Duff & Phelps or its related entities is not rendering legal, accounting or any other professional advice or services through presentation of this material. The information presented in this report has been obtained with the greatest of care from sources believed to be reliable, but is not guaranteed to be complete, accurate or timely. Duff & Phelps expressly disclaims any liability, of any type, including direct, indirect, incidental, special or consequential damages, arising from or relating to the use of this material or any errors or omissions that may be contained herein.