Equity Capital Markets Update

Q1 2014

OLSWANG

Contents

Recent Legal Developments and News

In this issue we look at some black letter issues concerning the contents of irrevocable undertakings under the Takeover Code and the impact of the Finance Bill 2014 on employee share schemes as well as getting an update on the Davies Review – Women on Boards - Annual Report 2014 and the increasing concerns surrounding cyber security measures amongst listed and quoted companies and efforts to increase awareness and readiness in light of the November 2013 launch of the FTSE 350 Cyber Governance Health Check Tracker.

Your feedback is always greatly appreciated and if you have any thoughts as to what you would like to see covered in the next edition of Olswang LLP's ECM Update please do get in touch with Andrew Stott (andrew.stott@olswang.com) or your usual contact.

Takeover Panel clarify terms permitted to be included in directors' irrevocable undertakings

Prior to the autumn of 2011, the trend in public M&A had been for bidders to seek ever more certainty about their ability to execute a transaction. This entailed, amongst other things, obtaining sweeping and restrictive assurances from the target company in relation to the level of assistance and facilitation to be given to the bidder to ensure a successful completion.

The Panel on Takeovers and Mergers (the "Panel") sought to put a stop to these arrangements as part of the changes that it made to the City Code on Takeovers and Mergers (the "Code") on 19 September 2011. In particular, implementation agreements and any other form of "deal protection measure" agreed to by the target company were prohibited.

Since then, however, certain bidders have attempted to gain some equivalent protections through irrevocable undertakings entered into by shareholders of the company who are also directors. Irrevocable undertakings from shareholders are not prohibited deal protection measures, provided that those shareholders who were also directors did not give those irrevocables in their roles as directors.

The Panel has now issued guidance about the boundaries of what is permissible. As a result, it is now clear that the following restrictions or commitments (amongst others) may not be included in the irrevocable undertakings signed by shareholders of a target company who are also directors:

- Not to solicit competing offers
- To recommend the offer to the shareholders
- To vote in favour of the offer in a board meeting
- To provide due diligence information to the bidder
- To conduct the target company's business in a particular manner

The Panel has also usefully summarised provisions that it would accept as being permissible:

- An undertaking not to dispose of shares
- An undertaking to make an election for a particular type of consideration
- A commitment to give warranties in relation to share ownership

There is no substantive change in the law, but the note represents useful guidance for shareholder-directors in their attempts to resist onerous restrictions, which they may feel (notwithstanding the usual "fiduciary duties" carve out) push the target company too far down the path to a particular transaction.

For further information, contact Edward Heaton at edward.heaton@olswang.com or on +44 20 7067 3808.

The Finance Bill 2014 – further changes made to employee share plans

The Finance Bill 2014, published on 27 March 2014, contains nearly 100 pages of new legislation relating to employee share plans. The majority of the changes came into effect on 6 April 2014 (assuming that the Finance Bill successfully makes its way through Parliament and receives Royal Assent). Companies may need to take action to ensure that their share plans are up-to-date and are being administered correctly, particularly given that this year's changes come on top of the significant changes introduced by last year's Finance Act. We consider below the implications.

Implementing new "approved" share plans

One of the most significant changes to have been introduced on 6 April 2014 is that new Company Share Option Plans (CSOP), Sharesave Schemes (SAYE) and Share Incentive Plans (SIP) will no longer require prior approval by HMRC. Instead, companies will need to "self-certify" any new plans. Whilst this will undoubtedly reduce the amount of time it takes to implement a new plan, companies will need to take greater care to ensure compliance as HMRC will no longer provide prior confirmation and fines will be imposed for breaches.

Online administration

With effect from April 2015, companies must submit HMRC's annual returns for their employee share plans (including Forms 34 (SAYE), 35 (CSOP), 39 (SIP) and 42 (other plans)) online. In preparation for this, companies must register each of their plans with HMRC before 6 July 2015. As the ability to register plans is already available, it is recommended that this is done by companies as soon as they are able.

This year's annual returns (for the 2013/14 tax year) must still be filed in paper form. These can be found here. However, registration of new plans, and filing of annual returns for 2014/15 onwards must be done through the "PAYE Online" portal on HMRC's website at www.online.hmrc.gov.uk.

Increased limits for SAYE and SIP

With effect from 6 April 2014:

- the monthly saving limit for SAYE increased from £250 to £500;
- the maximum 'free share' award under a SIP increased from £3,000 to £3,600; and
- the annual investment limit for 'partnership shares' under a SIP increased from £1,500 to £1,800.

Companies wanting to take advantage of the new statutory limits will need to make sure that their plan rules automatically cater for the higher limits. Equally, companies who do not wish to offer the increased saving opportunities to employees (for example, due to concerns about accounting costs and/or dilution limits) must take care to restrict their awards.

Are your plans up-to-date?

The Finance Act 2013 introduced a number of changes that applied automatically to CSOP, SAYE and SIP plans (see our Olswang blog here) and the Finance Bill 2014 proposes further automatic changes, largely to reflect the fact that advance approval from HMRC will no longer be required to amend share plans or adjust awards following certain changes to a company's share capital. Whilst there is no obligation to do so, companies should consider updating their plans to ensure that they reflect current law.

One particular issue to note is that, for all options granted under a CSOP on or after 6 April 2014, the legislation now stipulates a minimum level of information that must be provided to option holders at the time of grant. All companies should, therefore, ensure that their CSOP award documentation does comply with this new requirement.

Do your plans take advantage of new optional features?

In order to take advantage of the other optional features introduced under the Finance Bill 2014, companies will need to amend their existing plans. The optional features include:

- permitting the introduction of forfeiture provisions for 'partnership shares' and 'dividend shares' under a SIP (although, in practice, listed companies are unlikely to want to introduce this feature);
- where a takeover may otherwise cause the loss of tax-beneficial treatment, allowing SAYE and CSOP options to be exercised up to 20 days before a takeover event without losing the tax-beneficial treatment; and
- extending the definition of a 'takeover' in SAYE and CSOP plans to include certain overseas reorganisations (again, we await further guidance from HMRC as to the circumstances in which this may be necessary but it may be of assistance to companies registered outside the UK).

Internationally mobile employees

Although they will not come into effect until 6 April 2015, the Finance Bill 2014 proposes two changes that will affect internationally mobile employees:

- an extension of the availability of corporation tax relief for share options or other awards to those employees employed by a company that is outside the scope of UK corporation tax but where the employee also works for a company within the scope of UK corporation tax; and
- reform of the taxation of options held by employees moving to, or away from, the UK, ensuring that UK tax is levied on the proportion of the option gain that reflects the time spent in the UK during the vesting period.

For further information, contact Andrew Quayle at andrew.quayle@olswang.com or on +44 20 7067 3739.

Women on Boards 2014 – an update

On 26 March 2014 Lord Davies of Abersoch published the third annual progress report into Women on Boards. Three years on from the first ground-breaking review in 2011, Lord Davies and his steering group are reporting a growing number of women in decision-making roles.

2011-2014

The Davies Review Annual Report 2014 shows that women now account for 20.7% of overall board directorships in the FTSE 100 – up from 12.5% in 2011. There now remain only two all-male boards in the FTSE 100.

Notable developments in the last three years include two new FTSE 100 female Chief Executives being appointed at Severn Trent and the Royal Mail Group; the appointment of the second ever female Lord Mayor of the City of London; Lloyd's of London appointing their first female Chief Executive; and Lloyds Banking Group pledging that 40% of its top 5,000 jobs will be occupied by women within 6 years.

Lord Davies reports a "growing recognition" of the social and economic benefits of having more women on boards. Gender equality in business allows companies to:

- "improve performance at Board and business levels through input and challenge from a range of perspectives";
- "access and attract talent from the widest pool available";
- "be more responsive to the market by aligning with a diverse customer base, many of whom are women"; and
- "achieve better corporate governances, increase innovation and avoid the risks of 'group think'".

Lord Davies commends changing business practices, including the development of a whole new industry aimed at supporting women through their career progression and substantial developments by organisations such as Lloyds Banking Group, Barclays and Diageo. Initiatives such as 'Think, Act, Report', the UK Corporate Governance Code and the Voluntary Code for Executive Search Firms have been widely adopted.

Reaching targets

In 2011 Lord Davies recommended that FTSE 100 boards should aim for a minimum 25% female representation on their boards by 2015, which in practical terms means that fewer than 50 women need to be appointed to FTSE 100 boards in the next 18 months for the UK to meet this milestone. Such an achievement would double the percentage of women on boards since 2011 and is, according to Lord Davies, a target which "can clearly be achieved".

"*The voluntary approach is working and companies have got the message that better balanced boards bring real business benefits. We are finally seeing a culture change taking place at the heart of British business. However, the eyes of the world are on us as we enter the home straight. They are judging us*

as to whether the voluntary approach, rather than regulation, will work – we need to now prove we can do this on our own."

Legal intervention?

Lord Davies points out that the UK's voluntary, business-led approach is under intense scrutiny from European partners, regulators, investors and other stakeholders, while countries such as Germany have already chosen the legislative route. German companies are required to allot 30 percent of their non-executive board seats to women from 2016 or leave the positions unfilled. Meanwhile Norway, a non-EU member, imposed a 40 percent quota in 2003 - a target reached in 2009. Norwegian companies can be liquidated if they fail to reach the target.

The European Parliament voted in favour of legal quotas last November but the European Council reached deadlock on the matter. Failure by the UK to achieve the voluntary targets would raise the prospect of legal intervention by Government or from the European Union. With the spotlight on British business, Lord Davies asks the UK to prove that it can deliver real change in this area without legislative measures.

Lord Davies's report can be read in full here.

For further information, contact Marian Ang at marian.ang@olswang.com or on +44 20 7067 3785.

Cyber Security: concerns, new legal obligations and practical advice

In recent years many high profile companies have found themselves the victims of security breaches. PwC estimates the cost to be between £450,000 and £850,000 for a large organisation's single most serious breach in a year, not to mention the unquantifiable reputational damage which can affect the share price but can also impact customer loyalty and brand value.

FTSE 350 Cyber Governance Health Check Tracker

In November 2013, the Government published the FTSE 350 Cyber Governance Health Check Tracker, an aggregated tracker, assessing levels of cyber security awareness and activity across the FTSE 350. The tracker is the first of two phases, the second being a diagnostic phase, building on the results of the tracker. Results so far suggest that most executives are aware of the importance of cyber security and the threat of breaches (64% of Chairmen think their Board colleagues take cyber risk very seriously), but an alarming minority have undergone formal training (75% of respondents had not undergone any relevant training in the preceding year). BIS has drawn attention to this disparity, citing the fact that only 14% of FTSE 350 companies regularly consider cyber threats, although 62% take it very seriously.

New legal obligations to report cyber attacks

EU legislators published draft legislation in response to the threat posed by cyber attacks in February 2013, in the form of the Network and Information Security Directive (NISD). The NISD has progressed part-way through the EU adoption process, with the revised text being approved by the European Parliament on 13th March 2014. However, it still needs to be agreed by all three EU institutions so we are unlikely to see practical implementation at national level any earlier than 2016.

The NISD aims to 'ensure a high common level of network and information security' across the EU. The Directive applies to operators of infrastructure that are 'essential for the maintenance of vital economic and societal activities', including those in the financial, transport, health and energy sectors, in addition to certain online services such internet exchange points (but not e-commerce platforms). If an organisation is a market operator, its future obligations are proposed to include:

- **Cybersecurity measures:** taking 'appropriate and proportionate technical and organisational measures to detect and effectively manage the risks posed to the security of the networks and information systems which they control and use in their operations';
- **Notification:** notification obligations which involve notifying the appointed competent authority, without undue delay, of incidents which have a significant impact on the continuity of the core services they provide. Factors to determine 'significant' include number of users affected, duration, and geographic spread;
- **Information sharing:** the creation of a cooperation network between member states to share information and volunteer early warnings of breaches. The most recent version of the text also states that listed companies should voluntarily make cyber incidents public in their financial reports;

- **Cyber audits:** compliance with binding instructions from the competent authority, including providing evidence of effective implementation of security policies such as undertaking and making available an audit. The frequency and severity of this obligation is tailored according to the 'criticality' of the organisation; and

- **Technical standards:** member states are to encourage the use by businesses of international interoperable standards/specifications.

The proposed legislation is similar in scope to the recently published US Framework. However the US regime will be voluntary (an approach which is preferred by the UK), whilst the NISD imposes mandatory obligations on market operators.

The draft General Data Protection Regulation is also still awaiting final approval, and will introduce mandatory reporting of data breaches without undue delay to the supervisory authority and also to any individual who is substantially adversely affected. In addition, it will raise fines for data breaches from the current £500,000 available to the UK ICO, potentially up to the greater of €100,000,000 or 5% of global turnover.

Cyber Security in Corporate Finance

In addition to the FTSE 350 Cyber Governance Health Check discussed above, the ICAEW, with contributions from the London Stock Exchange amongst others, released a report on Cyber-Security in Corporate Finance in January 2014.

This report aims to give practical advice to organisations involved in corporate finance transactions – with multiple parties and professional advisers, and the multitude of data increasing cyber vulnerability. Corporate finance transactions are defined as 'those where an organisation's capital structure may be changed to develop, acquire or dispose of elements of that business'.

The publication details six phases of a transaction and highlights the vulnerabilities to cyber threat. These phases are:

- **Phase 1: Preparation.** Advice includes limiting the number of people involved in this opening stage, because 'the very act of putting information together may alert others that a transaction is imminent if information regarding the transaction is not secured'.

- **Phase 2: External Advisors.** The report advises on the importance of keeping track of who has what information, and ensuring that the advisors have similar security principles to protect the transaction data.

- **Phase 3: Initial Approaches.** At this stage, confidentiality agreements and secure data stores should be used, alongside the continuing principles of limiting who knows what information on a 'need-to-know' basis, and ongoing monitoring of access to data.

- **Phase 4: Disclosure & Due Diligence.** Large volumes of information are being made available, potentially to many groups of people. At this point, information about different organisations, such as customer and supplier data, is being put at risk. Therefore the publication advises considering the most appropriate format for the information. Note at the due diligence stage, parties should enquire about the cyber security practices of the target, and who is in charge of them.

- **Phase 5: Agreeing the Financing Terms.** The report advises considering the use of confidentiality agreements, and whether some information is best stored in an offline format due to the threats posed by virtual data rooms which organise highly confidential information – therefore making them easy to navigate if a hacker should gain access. Tips for data rooms include avoiding disclosing personal information unless necessary, limiting third party information, and having a staged release of information.

- **Phase 6: Completion.** At this stage, knowledge of the transaction may have become public – heightening the chances of a cyber-attack. As a result, continuous monitoring of access to the documents is crucial, and careful consideration must be taken when deciding the method of transferring funds.

Practical Steps

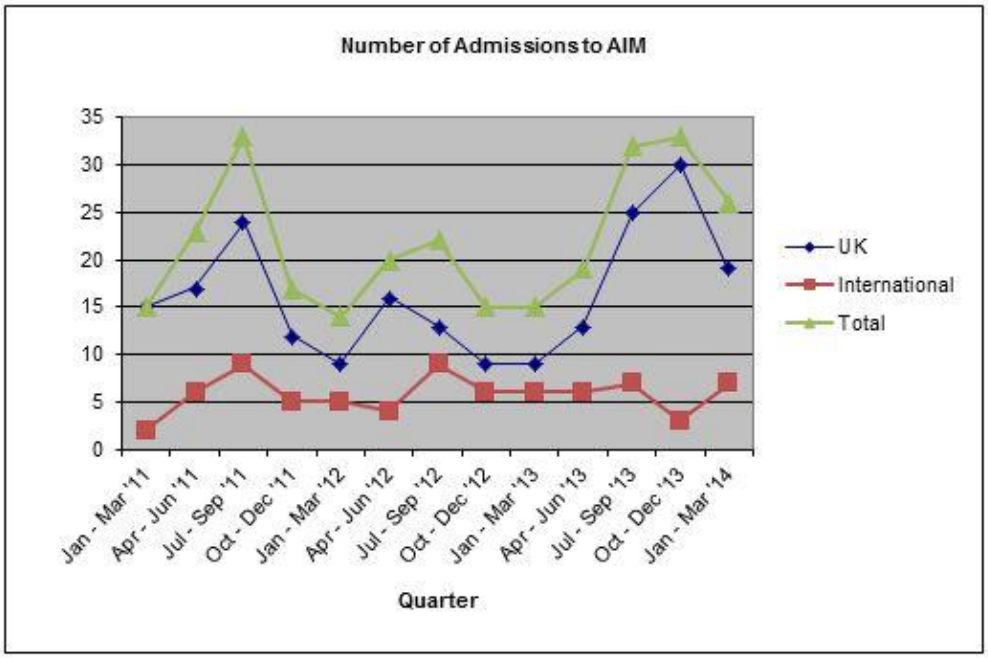
The statistics surrounding cyber threats are hard to ignore. Cyber security should be a high priority, Board level issue. Organisations should carry out security testing, train their employees and follow the wealth of guidance now available, to avoid becoming the next breach in the headlines.

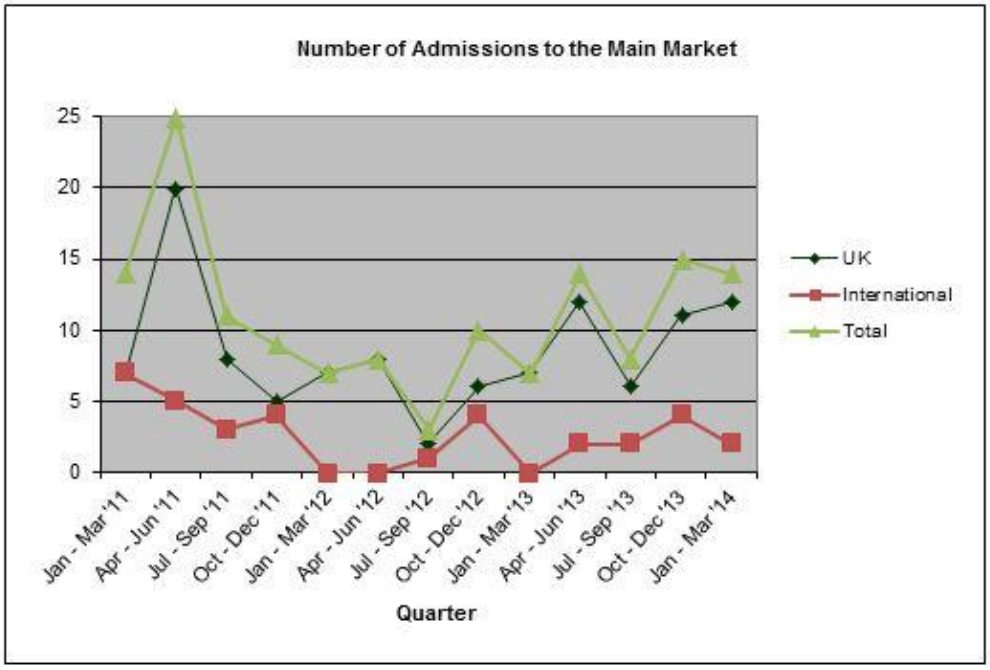
For further information, contact Lucy Berry at lucy.berry@olswang.com or on +65 9770 0337 or Katharine Alexander at katharine.alexander@olswang.com or on +44 207 067 3560.

Market Overview

NUMBER OF ADMISSIONS TO AIM AND THE MAIN MARKET

UK admissions to AIM have dropped by a third since the last quarter, with a less marked decrease occurring on the Main Market. International admissions on AIM have risen to the same number recorded six months ago whereas admissions on the Main Market have halved since the last quarter.

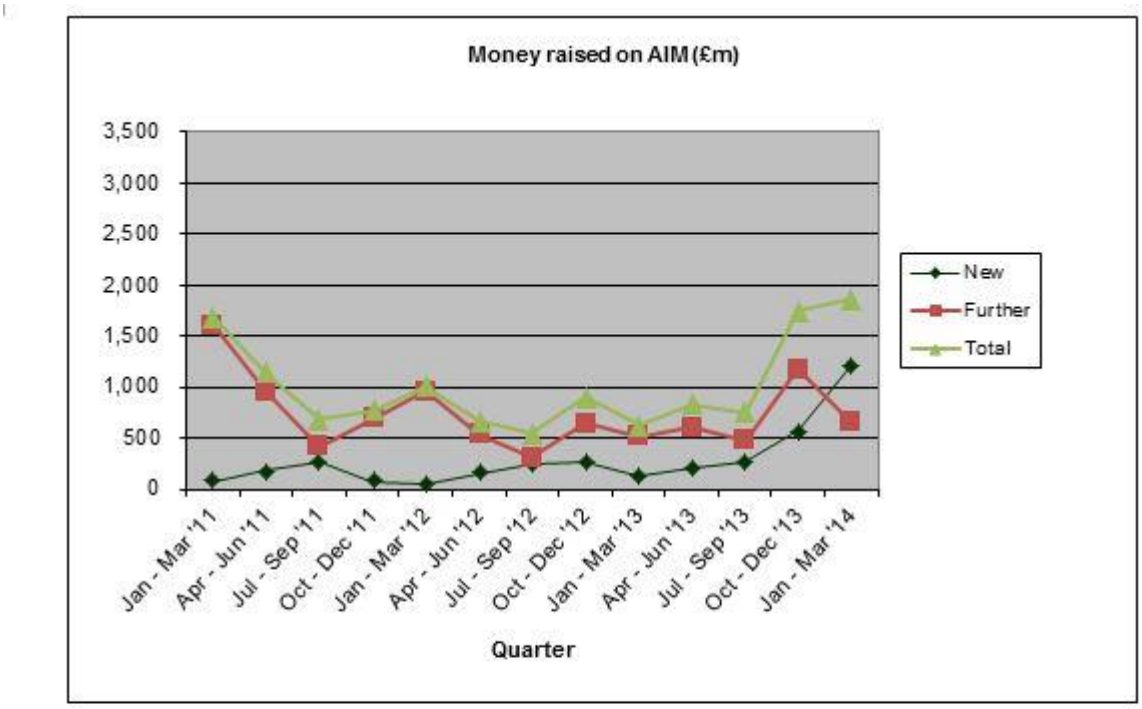


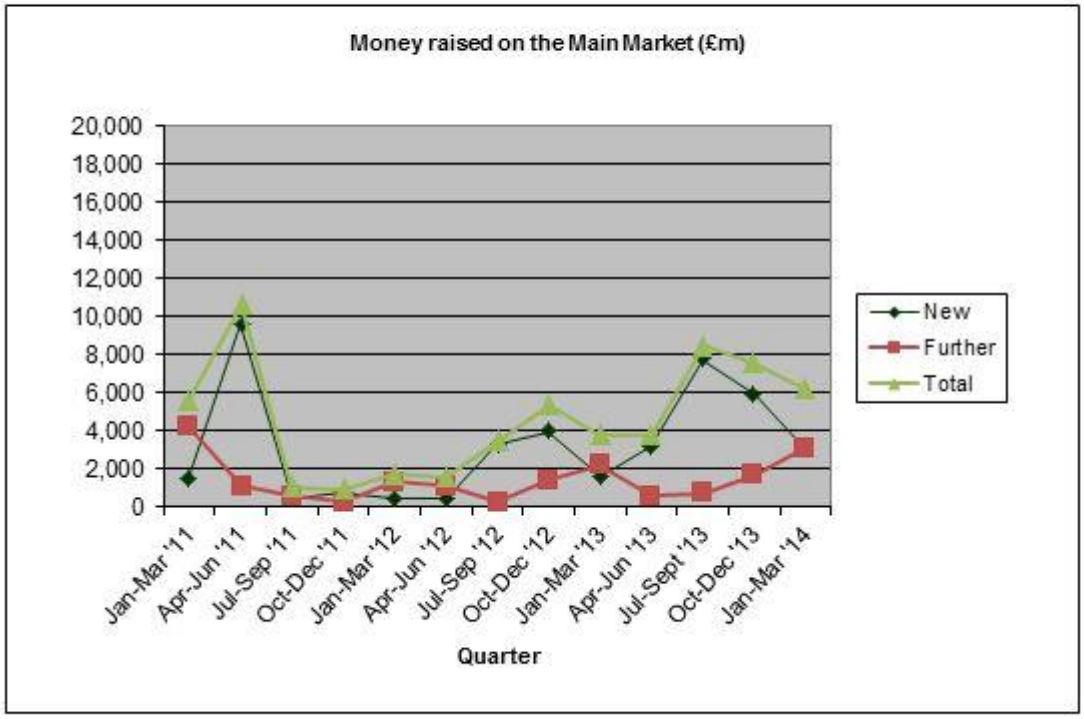


Source of data: London Stock Exchange

FUNDRAISING ACTIVITY ON AIM AND THE MAIN MARKET

Fundraising activity on AIM during Q1 showed a marginal increase but only due to the noticeable rise in the amount raised from new issues. In contrast, there was a sharp decrease in monies raised on secondary issues on AIM. Monies raised on the Main Market decreased since fundraising from new issues nearly halved since the last quarter.





Source of data: London Stock Exchange

Key Contacts

Azlinda Ariffin-Boromand
Partner
+44 (0)20 7067 3401
azlinda.ariffin-boromand@olswang.com

Paul Blackmore
Partner
+44 (0)20 7067 3468
paul.blackmore@olswang.com

Louis Glass
Partner
+44 (0) 20 7067 3347
louis.glass@olswang.com

Paul Guite
Partner
+44 (0) 20 7067 3465
paul.guite@olswang.com

Stephen Hermer
Partner
+44 (0)20 7067 3459
stephen.hermer@olswang.com

Simon Morgan
Partner
+44 (0)20 7067 3444
simon.morgan@olswang.com

David Roberts
Partner
+44 (0)20 7067 3537
david.roberts@olswang.com

Andrew Stott
Partner, Olswang Asia LLP
+65 9232 5326
andrew.stott@olswang.com

Anthony Waller
Partner
+44 (0) 20 7067 3461
anthony.waller@olswang.com

Robert Willis
Partner
+44 (0) 20 7067 3398
robert.willis@olswang.com

Max Audley
Of Counsel
+44 (0)20 7067 3484
max.audley@olswang.com

OLSWANG

Berlin	+49 (0) 30 700 171 100
Brussels	+32 2 647 4772
London	+44 (0) 20 7067 3000
Madrid	+34 91 187 1920
Munich	+49 89 206 028 400
Paris	+33 17 091 8720
Singapore	+65 6720 8278
Thames Valley	+44 (0) 20 7067 3000

www.olswang.com