Legal Focus

DRIVING LIFELONG PROSPERITY

Summer 2017

SPOTLIGHT ON MANAGING CYBER CRIME

Welcome...

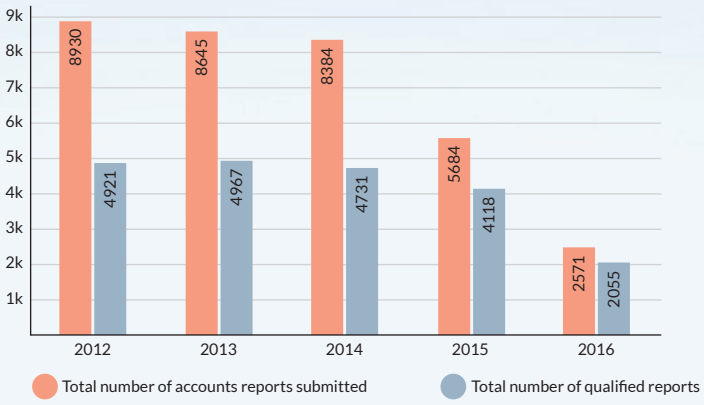
to the summer edition of Legal Focus. In this edition, we look at what to do when your cyber security is compromised or your clients' money vanishes, and the changes taking place in SRA Accounts Rules audits.

INSIDE

HAZLEWOODS
DRIVING LIFELONG PROSPERITY

DRAMATIC FALL IN THE NUMBER OF QUALIFIED ACCOUNTANT'S REPORTS

Back in 2012, almost 9,000 Accountant's Reports were submitted, of which 55% were qualified. The total number of submitted reports fell by about 6% in 2014, partly as a result of the SRA's decision that, from 1 November 2014, reports only needed to be submitted if they were either qualified or were 'Cease to Hold' reports. Even with the reduction in submitted reports, the proportion of Accountant's Reports that were qualified in 2014 remained fairly level, at 56%, as detailed in the table below.



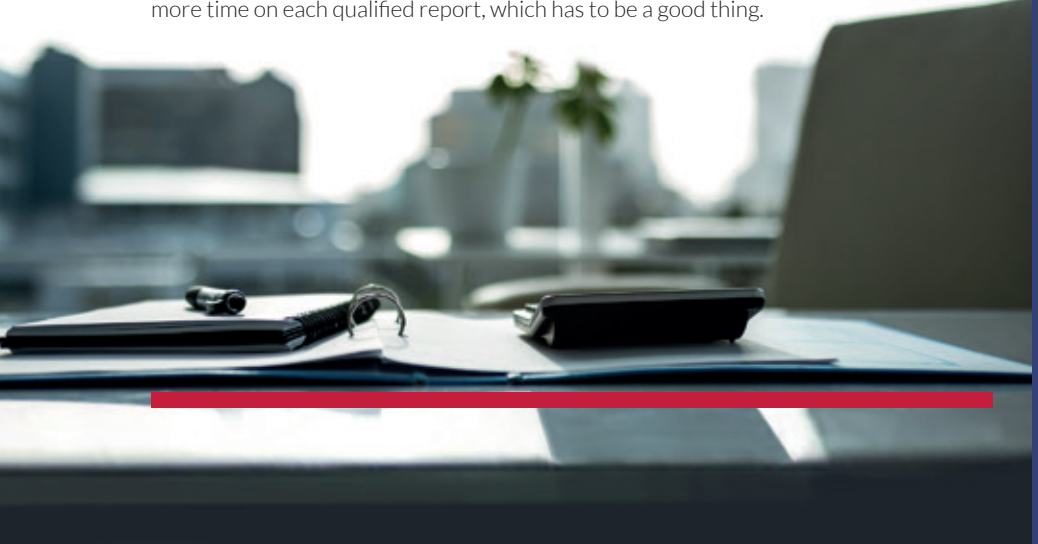
In 2015, the number of reports submitted to the SRA fell by almost a third, to 5,700. 4,100 (72%) of these reports were qualified, with the remaining 1,600 made up of Cease to Hold reports, or unqualified reports that had been submitted by Reporting Accountants, despite the changes in 2015.

In addition, approximately 1,000 practices no longer need an Accountant's Report as a result of the SRA's new exemption criteria.

Following changes to the types of breach that result in a qualified report, as detailed in the article on the new Reporting Accountant regime, the number of Accountant's Reports submitted to the SRA last year fell below 2,600; 80% of these were qualified. Whilst this represents a significant drop, the number of qualified reports is higher than the SRA anticipated. One explanation for this could be that some Reporting Accountants are still getting used to the changes, and are qualifying their reports for breaches that the SRA might consider 'trivial', just to be on the safe side.

Our expectation is that the number of qualified Accountant's Reports submitted to the SRA in 2017 is likely to fall still further, as accountants settle into the new regime. At the same time, our experience is that practices are now taking qualified reports more seriously than they used to when most were qualified and are putting more effort into addressing weaknesses in their systems and control procedures.

Finally, we have been contacted by the SRA several times recently in connection with qualified Accountant's Reports that we have submitted. Each time, the SRA has asked for additional information and an update on the breaches included in the Accountant's Reports. Prior to the November 2015 changes, we were rarely contacted by the SRA in connection with an Accountant's Report, despite submitting well over 100 reports each year. Clearly, the SRA is now spending more time on each qualified report, which has to be a good thing.



SRA HOT TOPICS

RESIDUAL BALANCES ON CLIENT ACCOUNTS

Practices need to be proactive in dealing with residual balances on a timely basis. Where the owner of the funds cannot be traced, balances less than £500 may be donated to charity without seeking permission from the SRA.

ACTING AS A BANK

This is one of the SRA's hot topics at the moment, and they really do frown upon practices receiving monies or making payments on behalf of clients which do not relate to the underlying matter or service being provided. There is lots of guidance about this on the SRA's website, including case studies.

In addition, the Office of the Public Guardian (OPG) has recently published practice note 02/2016 on the OPG's approach to solicitor client accounts, which sets out the OPG's approach to the use of client accounts to manage deputyship funds.

What do you do when disaster strikes?

Before Easter, we welcomed a panel of experts to provide an open forum at our Staverton office, where they were quizzed by our guests, keen to learn what actually happens when money disappears from your client account. It was a lively interaction, with real life case studies relayed by our IT expert Jake Hockley of Marclay Associates Limited, PI expert Brett Warburton-Smith of Lockton Companies LLP, and Banking fraud expert Andrew Barnett of Barclays Corporate and International Fraud Risk.

We heard how the use of the internet, social media sites and electronic messaging is still growing at an unprecedented rate, enabling us to operate our businesses in a virtual environment, often never physically meeting the people we communicate with. Whilst this does have many efficiency benefits, the culture change has facilitated a boom in social engineering, fuelling the exploitation of the natural human instinct to trust. Criminals are becoming increasingly clever at taking advantage of this.

Time after time examples were given of financial controls being overridden by individuals manipulated by fraudsters, often over a number of weeks, and tricked into divulging confidential information. The fraudsters were pictured as smartly dressed individuals operating from modern offices, not unshaven hoody wearers.

So, what should you do when the awful realisation dawns that your practice has been targeted and your clients' money has vanished, and in what order?

1. **Call your bank immediately.** As soon as the bank is alerted, further distribution of the stolen funds can be stopped. We heard that if this is within 20 minutes of the initial fraudulent transfer it may be possible to recover as much as 80% of the stolen money, but after 40 minutes this may be only 20%, or less.

2. **Call the National Fraud and Cyber Crime Reporting Centre on 0300 123 2040.** Cases can be investigated far more successfully, with large amounts of data, when cases are linked.

3. **Call your PI broker/insurer.** This triggers a claim under your PI policy for the loss to the client account. Your insurer will also have useful advice on protecting yourselves from further losses.

4. **Inform the SRA** on 0121 329 6827 or email at fraud@sra.org.uk. Do not delay doing this. The SRA will work closely with you to safeguard your clients' interests. It might also be able to assist in expediting the police involvement.

5. **Inform the client** whose money has been misappropriated, if this can be specifically identified. It should be possible to obtain early indications from your insurer and your bank as to the steps they are prepared to take to replace the funds. Under the SRA Account Rules 2011, it is your duty to remedy breaches; if the bank or insurer delays or refuses to replace the stolen funds, the SRA will insist the principals do so from their own funds, if they can of course.

Your cyber-security has been attacked! Don't panic!

Perhaps you are already executing a carefully crafted crisis response plan and know exactly what to do next? If not, read on and let us steer you in the right direction. Here are 5 steps that we have found to be a useful guide during the early phases of an incident:

1. **ASSEMBLE AN INCIDENT LEADERSHIP TEAM**
   This is normally a small internal team who hold senior managerial and budgetary responsibility, together with relevant subject matter experts who can feed information into the decision makers (e.g. IT Director). The team should hold an initial meeting and share as much information as is available about the incident. This would ideally be face-to-face, but a conference call is often the quickest approach and speed is critical.

2. **COMMUNICATIONS – INTERNAL AND EXTERNAL**
   Early consideration should be given to the impact the breach is likely to have on your practice. Do you need to formulate a media release, email (or other communication) to all clients, or maybe even press interviews? Do you need to think about informing all employees? Could employees help with the investigation and isolating the affected systems? It may, of course, be prudent to exercise an element of discretion, especially when you are still trying to ascertain the exact cause and scale of the breach; all of this should be a call for your incident leadership team.

3. **INVESTIGATE THE INCIDENT**
   Gathering information is key at this stage. It is important to validate that the breach is real, understand who is involved, where and when the incident occurred, exactly what happened and, if possible, what information or data has been affected.

4. **ISOLATE THE SYSTEM**
   It is important to eradicate the cause of the breach, either by taking servers offline, changing passwords for cloud services and/or speaking with the service provider to regain control of the affected systems.

5. **RECOVER**
   Once you are confident that the 'hole is plugged' and the possibility of a future breach has been removed, it is time to look at restoring 'business as usual'. With any form of cyber breach, you may feel that you lack the internal resources or specialist skills required to react effectively during an incident. If this is the case, then it makes sense for a professional cyber response team to be brought in to support you through these steps. Ideally, this team would be co-located with the in-house incident leadership team during the initial phase of an incident, but many early decisions and actions can be taken on a secure conference call with remote access to the affected party's IT systems.

Contribution by Jake Hockley
www.marclay.co.uk

The new Reporting Accountant regime 18 months on

From 1 November 2015, reporting accountants have needed to use their professional judgement to devise suitable work programmes to determine whether or not to qualify their Accountant's Reports. Furthermore, Accountant's Reports are now only qualified where material breaches are identified which are likely to put client money at risk. The SRA defines material as 'likely to arise as a result of an intention to break the rules and/or as a result of a significant weakness in the firm's systems and controls', i.e. something pretty serious.

So, how has the scope of our audit testing changed since then?

DETAILED PLANNING

The new rule 43A, 'work to be undertaken', gives guidance on the factors that Reporting Accountants might consider when deciding what audit work to carry out, such as the size and complexity of the practice, the nature of the work undertaken, the number of transactions, and amount of client funds held.

We have always considered these factors, and lots of others, but as a result of the new latitude, we now put more emphasis on identifying the key areas of risk, and documenting and understanding internal systems and controls at the planning stage of our work. Where we ascertain that reliance can be placed on the internal controls, our detailed testing can be reduced.

REVIEW OF THE BREACHES REGISTER

Note (ii) to Rule 43A suggests that Reporting Accountants should consider the numbers and types of breaches that the COFA has recorded during the year. Also, in their guidance on the type of factors that could lead to a qualified report, the SRA states that material breaches not reported to the SRA by the COFA should be reportable, and breaches that were not reported to the SRA on a timely basis might be reportable.

Clearly, we need to see the Breaches Registers for both of these points.

Some practices have concerns that giving their accountants access to their Breaches Register could result in them simply taking all of the points on the register and including them in the Accountant's Report. This is a valid concern, but we would never do this.

In fact, sometimes we do not ask to see the Breaches Register at all, provided we are happy that there is a register in place, and we know that there is an effective COFA.

RELIANCE ON STRONG INTERNAL CONTROLS

Where internal controls are seen to be effective, with plenty of segregation of duties to further reduce risk, we carry out detailed testing on those controls to ensure that they are working as expected, similar to the way that we do on a statutory financial audit. This usually involves walk-through tests (following a client transaction from start to finish, checking that each stage of the process was carried out and authorised in accordance with the practice's procedures). For example, checking a sample of bills to ensure that they were reviewed and approved before issue and checking that the internal IT policies are adhered to.

Where our testing shows that the documented controls are working, we are able to confirm compliance with the Accounts Rules in a different way, without carrying out as much detailed substantive testing.

TRANSACTIONAL TESTING AND CLIENT FILE REVIEWS

Our approach to testing payments and receipts, bills and transfers is largely unchanged. Sample sizes have generally remained in line with previous levels and are still determined by our assessment of the inherent risk of a practice not complying with the rules.

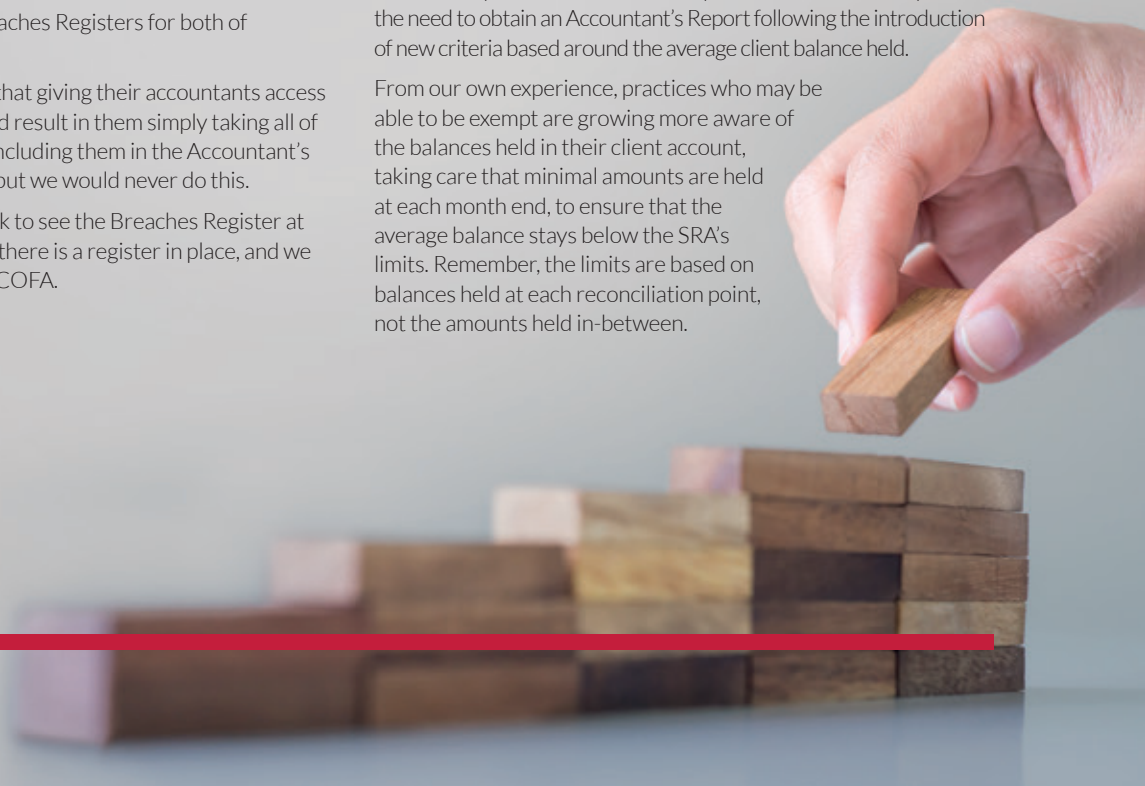
Unless there have been issues in previous years, we are usually able to reduce the level of testing of the client account reconciliations. Rather than looking at every unreconciled item on the reconciliation and ticking them to bank statements, we now focus on the larger or more unusual items.

The number of cheques issued by practices is falling and we have changed our testing to reflect this. As a result, far fewer paid cheques are requested from the bank, and sometimes none at all.

EXEMPTION FROM SRA AUDIT

The SRA's expectation was that 1,000 practices would be exempt from the need to obtain an Accountant's Report following the introduction of new criteria based around the average client balance held.

From our own experience, practices who may be able to be exempt are growing more aware of the balances held in their client account, taking care that minimal amounts are held at each month end, to ensure that the average balance stays below the SRA's limits. Remember, the limits are based on balances held at each reconciliation point, not the amounts held in-between.



STOP PRESS! CHANGES TO SRA ACCOUNTS RULES 2018 PUBLISHED

The SRA has now published a new version of the SRA Accounts Rules 2018, running to seven pages and 13 rules, updated for the following:

1. Money received in advance for the payment of fees and disbursements will continue to be client money, and should be held in client account until the point at which they are billed, i.e. no change from the current position;
2. Where the only client money that a practice holds is in respect of advance fees and disbursements then the practice can elect to hold the money in its office account, provided clients are informed upfront of where and how the money will be held;
3. The SRA has removed the reference to the practice's COFA being jointly and severally liable with the practice's managers (partners, members or directors) for compliance;
4. All payments from the Legal Aid Agency can in future be held in the office account, including money received for unpaid disbursements;
5. The SRA will no longer require a 'Cease to Hold' Accountant's Report when a practice ceases to hold client money (for example on a cessation), unless the SRA specifically requests one;
6. The SRA are proceeding with their proposals to allow solicitors to use Third Party Managed Accounts (TPMAs).

For the majority of practices, this is all good news, as it will mean that they can carry on as they always have, with no changes to systems and processes other than those they choose to make to take advantage of the increased flexibility in the rules. For example, practices will be able to come up with new timeframes and deadlines around the banking of client monies, transfers for costs etc., if they so wish.

The changes will also be good news for practices merging, converting to LLP or incorporating to a limited company, which will no longer need to have a separate 'Cease to Hold' audit, for a simple change in the client account title.

The new rules are likely to be effective from 1 November 2018. Watch out for news of our update courses for cashiers and COFAs, taking place during November and December 2017.

APPRENTICESHIP LEVY – A BLESSING IN DISGUISE?

From April 2017, practices with payroll costs over £3 million are subject to a new tax in the form of the apprenticeship levy. It is assessed at 0.5% of the payroll bill subject to National Insurance, so does not include amounts paid below the lower NI threshold. Each employer is entitled to a 'levy allowance' of £15,000 per annum, that is, the total liability arising on the practice in the year is reduced by £15,000, regardless of size.

However, it is not all bad news! Employers are entitled to claim back eligible, and pre-existing training costs. Indeed, there may be big wins if your practice spends more on training courses than it has paid in via the apprenticeship levy, then the government can fund up to 90% of the additional cost.

Legal sector apprenticeships currently available include:

→ Paralegal (2 years)
→ Chartered legal executive (5 years)
→ Solicitor (5-6 years)

Further information may be found at **www.gov.uk/government/publications/apprenticeship-standard-solicitor**

NEW ASSOCIATE PARTNER

We are delighted to announce that Andy Harris has been promoted to Associate Partner from 1 May 2017. Andy joined Hazlewoods as a trainee back in 1997 and has been a key member of our Legal Team ever since.

Congratulations are due to our tax specialists too. Karl Millward is promoted to Manager, Cheryl Thomas to Senior Associate and Kurt Lawrence to Associate.

Other promotions in the Legal Team go to Maria Smith, who is now a Senior Associate, and Emma Whittaker becomes an Associate.

JON CARTWRIGHT
Partner
01242 237661
jon.cartwright@hazlewoods.co.uk

PATRICIA KINAHAN
Partner
01242 237661
patricia.kinahan@hazlewoods.co.uk

ANDY HARRIS
Associate Partner
01242 237661
andrew.harris@hazlewoods.co.uk

HILARY EVANS
Director
01242 237661
hilary.evans@hazlewoods.co.uk

Windsor House, Bayshill Road, Cheltenham, GL50 3AT
Tel. 01242 237661 Fax. 01242 584263

www.hazlewoods.co.uk / @HazlewoodsLegal

HAZLEWOODS
DRIVING LIFELONG PROSPERITY