

Professional Indemnity Insurance
The hidden risks that
will impact law firms

August 2018



For those kept awake at night by the many risks facing the profession the release of the latest SRA's Risk Outlook 2018/2019 Report¹ sheds light on the key areas that law firms should be aware of and be taking action on.

Importantly, this year's report sees cyber security and claims management included in the top ten of key risk areas.

This article will focus on six of the main risk areas that were highlighted within the Report, these are:

Top Six Risks



Service Standards, in particular complaints



Information Security



Cyber Security



Protecting Client Money



Anti-Money Laundering



Managing Claims

Service Standards

According to the Report the most common complaints reported were related to delays, lack of competence and negligence which were made direct to law firms (known as first tier complaints).

Conveyancing work attracted the most complaints reported to the SRA and the Legal Ombudsman² and complaints to the Legal Ombudsman in relation to poor communication and delay have increased³.

Why is this an issue?

The standard of service expected of solicitors is very high. Furthermore, SRA Principle 5 states that you must provide a proper standard of service to your clients.

Key Actions

- Ensure that your client care information is clear and concise, with key areas highlighted and the firm's complaints procedure clearly accessible
- Manage your client's expectations about their options and keep them informed of progress
- Agree the services and the costs from the outset and keep clients informed on running costs
- Ensure that you can identify vulnerable clients and provide appropriate information and support suitable to their needs
- Complaints should be responded to promptly, fairly, openly and effectively

In summary, clients should be provided with a competent service, that is delivered in a timely manner and takes into account your clients' needs and best interests.

1. SRA Risk Outlook 2018/2019 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page>

2. SRA Risk Outlook 2018/2019 - page 53 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page>

3. Annual Report Legal Ombudsman 2017 - <http://www.legalombudsman.org.uk/?portfolio=annual-report-2016-17>

Information Security

Law firms handle vast amounts of client and sensitive information which is attractive to cyber criminals. Should this information fall into the wrong hands it can be harmful to both your clients' interests and your firm's reputation. Information breaches can arise in many ways and cyber crime is a common cause for such breaches, but it is important to remember written and verbal communications also carry a risk. A report on data security incident trends from the Information Commissioner's Office (ICO) shows that for all sectors for the first quarter of 2018 they received 284 reports of data being sent to the wrong person by email, post or fax.

"most common legal sector breaches are confidential emails and letters being sent to the wrong person, and lost or stolen paperwork"⁴.

The ICO have responded to the increased awareness and volume of reports of Data protection breaches by launching Personal Data Breach Helpline.

Cyber Security

An associated theme is the worrying rise in cyber security risk across the legal sector. The legal profession is attractive to criminals because law firms hold vast amounts of client money and personal data at any one time, both of which are clearly valuable assets to cyber criminals.

According to the SRA, 2017 saw a 52% rise in reported cyber crime incidents whilst £10.7 million of client money was reportedly lost to cyber crime, an increase from £9.4 million in 2016⁵.

Many of you will be aware of the types of cyber scams that the legal profession has seen and have been reported, but let's highlight the following:



CEO Fraud: also known as Business Email Compromise (BEC) or whaling. This arises when a cyber criminal pretends to be a CEO or senior manager within a law firm through hacking or purchasing a similar email address. The criminal will most likely order money to be transferred and/or facilitate tax fraud.



Identify Theft: bogus law firms or bogus branch offices hijack the identity of genuine law firms in order to carry out illegal activity such as deposit frauds, inheritance frauds and investment fraud. Such events damage the reputation of the legal profession.



Malware: this is software that is designed to disrupt/damage a computer system. Malware includes viruses and ransomware programs. These programs attack your device, stopping it from working, stealing your data; or demanding a ransom in return for a decryption key.



Phishing and Vishing: this is the fraudulent practice of using emails or telephone calls to obtain confidential information, such as bank details and credit card numbers from individuals by purporting to be from a reputable company for example: your bank or a service provider.

Key Actions

- Implement policies and procedures that address
- How and when sensitive information should be taken out of the office
- Identify clear reporting lines so employees know who to report such matters to
- With the increase of agile working, ensure that you have devised and communicated a Working From Home Policy that also incorporates the handling of sensitive documents
- Ensure all members of staff are appropriately trained to be alive to the risks from cyber crime and scams
- A protocol for dealing with lost or stolen documents, laptops and smartphones. This ideally should be set out within your firm's Business Continuity Plan
- Implement a Clear Desk Policy

What can you do to protect electronic data?

- Do not open attachments or click on links contained within an email unless you are certain that they are legitimate and/or are from trusted sources
- Ensure that your anti-virus and anti-malware software is up to date
- Keeping data regularly backed up to help recover from a cyber event such as a ransomware attack and test the back-ups regularly to check its efficacy
- Use a VPN when working offsite
- Do not use public Wi-Fi to access secure information; and password protect your data and change them regularly

Whilst it is important to protect your firm's electronic data, protecting physical data is equally as important, especially if working remotely such as on the train. Be mindful of not sharing sensitive information when talking on the telephone in public. Implement a Clear Desk Policy and make sure that confidential waste is processed correctly and ensure that both the firm and your supplier are compliant with the data protection legislation.

Education and awareness plays a key role in information security. You should ensure that everyone, from the executive team down receives training on information security and cyber risk. Many firms now regularly test their team's knowledge and awareness in these areas and there are resourceful websites that firms can visit to seek further information and guidance on this area.

The ICO website has helpful guidance and information for business of all sizes and there is the Government based scheme Cyber Essentials, <https://www.cyberessentials.ncsc.gov.uk/> which is aimed at providing advice about cyber risk.

The National Cyber Security Centre published a report last month examining the cyber threat to the UK legal sector⁶. This gives handy tips on how UK law firms of all sizes can protect themselves from common cyber threats.

4. SRA Risk Outlook 2018-2019 page 9 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page>

5. SRA Risk Outlook 2018-2019 page 13 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page>

6. The National Cyber Security Centre Report July 2018 - <https://www.ncsc.gov.uk/legalthreat>



Protecting Client Money

Another risk identified in the Report concerns the protection of client money. The misappropriation of client funds is a significant risk to law firms and by ensuring that you have the appropriate controls and systems in place you can mitigate the risk of monies being misappropriated by third parties.

Those familiar with conveyancing transactions will note the high profile appeals of *Dreamvar (UK) Limited v (1) Mishcon de Reya (a firm) and (2) Mary Monson Solicitors Limited [2016] EWHC 3316 (Ch)* and *P&P Property Limited v. (1) Owen White & Catlin LLP and (2) Crownvent Limited t/a Winkworth [2016] EWHC 2276 (Ch)*, when client money of genuine buyers was targeted by fraudsters in a property scam. These cases illustrate that conveyancing transactions are a particular risk and attractive to criminals given the vast sums involved.

The SRA restated in their 2018-2019 report that the most commonly reported method for the misappropriation of client monies was email modification fraud (2018, p. 13). The fraud occurs when criminals impersonate a genuine person engaged in a property transaction. The criminal hacks into that individual's email system, either intercepting the email and/or forging emails from it. The SRA reported that there was an 85% increase in thefts of property deposits in 2016 using this method⁷ and in the first quarter of 2018, email fraud had risen to 71%⁸.

How does it work?

Criminals contact the solicitor using a stolen or falsified email address, purporting to be the client and asking for the client's bank details to be changed. Cases have also been reported where the criminal impersonates the law firm, informing the client that the firm had changed its bank details. On receiving the email, the client unwittingly sends the deposit monies and purchase monies to the fraudster's bank account. This is more commonly known as "Friday Afternoon Fraud".

How to protect your firm?

You should implement appropriate systems and controls for accessing client money, including who, how and when it can be accessed. These measures should include the appropriate vetting, supervision and training of staff.

There are additional measures that you can consider implementing to manage such risks.

Key Actions

- Exchanging bank details with all parties at the start of the transaction
- Confirm that your bank details will not change on your email footer
- Include information in your Client Care Letter and Terms of Engagement, informing clients that your bank details will not change
- Provide appropriate training to staff
- Protect client information
- Consider using systems that offer lawyer checking services, to verify bank information for third party law firms

7. SRA Risk Outlook 2017/2018 page 29 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2017-2018.page>

8. SRA Risk Outlook 2018-2019 page 13 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page>

Money Laundering

The UK Government's National Risk Assessment of Money Laundering and Terrorist Financing, published in October 2017 (2017 NRA)⁹ identifies the legal profession to be at a high risk of exploitation for money laundering. In order to make it difficult for criminals to carry out such activities, solicitors must comply with their regulatory and legislative obligations to prevent money laundering and terrorist financing, including:-

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017)¹⁰
- Terrorism Act 2000
- Proceeds of Crime Act 2002
- Criminal Finances Act 2017
- SRA Code of Conduct 2011

Key Actions

- Provide updated training for all relevant staff members to make sure they are aware of the changes under the 2017 MLR
- Implement a firm-wide risk assessment to include steps you have taken to mitigate the risks of money laundering and terrorist financing that you face
- In addition to the mandatory firm-wide risk assessment you should also implement a client/matter risk assessment. This should inform the way you carry out your client due diligence depending on the result and ongoing monitoring. The process for carrying out this risk assessment should be detailed in the firm-wide assessment
- Take a risk based approach to each client matter and conduct appropriate client due diligence
- Ensure you check source of funds (where appropriate)
- Ensure that your client account is not exploited or used as a banking facility for clients¹¹

The SRA have reported that there has been a "67% increase in money laundering reports over the last 18 months"¹².

The SRA also are coming down hard on solicitors who are permitting their client accounts to be used as banking facilities in contravention of the SRA Accounts Rules 2011. In the last 12 months, the SRA has prosecuted 20 solicitors and three law firms at the Solicitors Disciplinary Tribunal for breaches in this area. Three solicitors have been struck off and two more suspended, and fines have been levied of £763,000, including the highest fine ever imposed in the sum of £500,000¹³. To assist law firms avoid the improper use of the client account, the SRA has produced guidance which includes 11 case studies¹⁴.

The SRA's Thematic Review of Preventing Money Laundering and Financing of Terrorism in March 2018 illustrated that "most firms visited where taking the appropriate steps to understand and reduce the risk of money laundering and to comply with the regulations". However, there were examples of:

- A lack of record keeping of decisions made
- Firm-wide risk assessments not being implemented
- Improvements required for both processes and practice

The SRA have stated that in the "most serious cases ... they have taken firms into their disciplinary process"¹⁴.

MLROs have a duty to ensure law firms are compliant with their regulatory and legislative obligations and consideration should be given to the following:

- Ensure policies and procedures are regularly reviewed and updated and any changes are communicated to staff
- Ensure record keeping procedures are in place
- Carry out regular internal audits and compliance reviews
- Submit suspicious activity reports whenever they detect suspicious activity

The findings of the 2017 NRA, which identifies the legal profession to be a high risk of exploitation of money laundering, has resulted in the introduction of a new Anti-Money Laundering Regulator, The Office for Professional Body Anti-Money Laundering Supervision (OPBAS). OPBAS operates within the FCA's existing governance and oversees the work of the 25 individual supervisory bodies appointed by HM Treasury. It is in essence the regulators regulator. OPBAS intends to improve co-ordination and overall standards of supervision, making sure that supervisors and law enforcement agencies work together effectively.

Another measure to help raise awareness of the warning signs of money laundering is the Government 'Flag It Up' campaign which is aimed at assisting the legal profession and accountants to identify potential red flag warning signs of money laundering. Examples of red flag indicators of money laundering could include:



Clients: are they overly secretive or evasive? Do they refuse to provide all the necessary information and documents? Are there inconsistencies in what they say?



Funds: is the amount and source of funds unusual? Is the client using multiple bank accounts or foreign accounts without good reason? Are the funds received from or sent to high-risk countries?



Transactions: are there discrepancies in client transactions? Is the client involved in transactions which do not correspond to their normal professional or business activities? Are the transactions unusual because of their size, nature, frequency, or manner of execution?

9. HM Treasury and Home Office (2017). UK National Risk Assessment of Money Laundering and Terrorist Financing. Retrieved from HM Government website: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf

10. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. http://www.legislation.gov.uk/uksi/2017/692/pdfs/uksi_20170692_en.pdf

11. SRA Risk Outlook 2018/2019 page 43 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page>

12. SRA Risk Outlook 2018/2019 page 41 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page>

13. The Law Society Gazette 7 August 2018 - <https://www.lawgazette.co.uk/news/sras-message-to-firms-stop-offering-banking-facilities-to-clients/5067197.article>

14. <https://www.sra.org.uk/solicitors/code-of-conduct/guidance/case-study/improper-use-client-account-banking-facility.page>

15. SRA Preventing Money Laundering and Financing of Terrorism A thematic review March 2018 page 7 and 8 <https://www.sra.org.uk/sra/how-we-work/reports/preventing-money-laundering-financing-terrorism.page>

Managing Claims

The SRA have identified particular concerns relating to claims arising out of holiday sickness, payment protection insurance and personal injury. The main risk that firms should be aware of is that many of these types of claims are not genuine.

The SRA have investigated and taken action against firms where there has been links with claims management companies and payment for referral of such claims.

Payment Protection Insurance Claims have been highlighted as a risk factor, according to the Report¹⁶,

“Firms are failing to meet high professional standards when bringing claims for mis-sold PPI and other financial products”¹⁷.

What can you do to protect your firm?

- Ensure that you whilst taking clients instructions, you do not compromise your duty to the court and the proper administration of justice
- Ensure that you comply with any legislation relevant to the claim.
- Ensure that you provide a proper standard of service to your clients

Law firms should regularly review their approach to identifying, monitoring and managing risks to their businesses and by considering the mitigating factors detailed above should provide assistance with this task.

16. SRA Risk Outlook 2018-2019 page 35 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page>

17. SRA Risk Outlook 2018-2019 page 37 - <https://www.sra.org.uk/risk/outlook/risk-outlook-2018-2019.page>

For more information contact:

Nicola Anthony
Lead Associate: FINEX Global

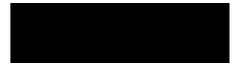
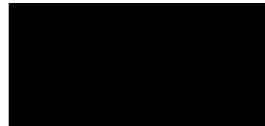
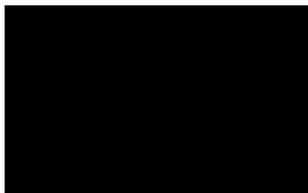
Willis Towers Watson
11th Floor,
51 Lime Street
London EC3M 7DQ

D: +44 2031248910

M: +447880781202

E: Nicola.Anthony@WillisTowersWatson.com

willistowerswatson.com





About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees in more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.



willistowerswatson.com/social-media

Willis Limited, Registered number: 181116 England and Wales.
Registered address: 51 Lime Street, London, EC3M 7DQ.
A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority for its general insurance mediation activities only.

Copyright © 2018 Willis Towers Watson. All rights reserved.
WTW-FINEX-280107/08/18

willistowerswatson.com

Willis Towers Watson