Editor's Note

ESSAR Insurance Services Limited, Managers of the Professional Indemnity Scheme in collaboration with Panel Solicitors Johnson Stokes & Master, issue this quarterly bulletin to highlight risk management issues learned from their handling of claims.

Ethical and Legal Challenges in the Era of Remote Work

The COVID-19 pandemic had a transformational impact on workplace dynamics. The prevalence of remote work technologies, availability of high speed reliable internet connections and increased mobility have accelerated the adoption of remote work across various industries, and the legal profession is no exception.

Remote work offers flexibility and convenience, but it also presents unique ethical and legal challenges for solicitors in discharging their duty to serve clients in a conscientious, diligent, prompt and efficient manner (Principle 6.01(b) of Hong Kong Solicitors' Guide to Professional Conduct ("**Guide**")). The modern workflow also results in solicitors using mobile devices, and even messaging apps, more frequently. Moreover, the expectation of higher levels of service and responsiveness has added pressure on solicitors to meet their clients' demands no matter where they are or whether they are on leave. This bulletin explores the challenges of remote or hybrid work arrangements and provide practical suggestions on how to manage risks arising from them.

1. Confidentiality and Data Security

Solicitors have a duty to maintain the confidentiality of client information, as outlined in Chapter 8 of the Guide. Remote work increases data security risks in a number of ways, such as accessing firms' intranet or data using personal devices, connecting to insecure networks or losing laptops and flash drives in public spaces. Such data security malpractice might result in unauthorized access to confidential information. Threat actors are acutely aware that law firms hold highly confidential information (and handle large sums of money) which make them tempting targets and susceptible to ransom demands. The impact of a significant breach is crippling in terms of lost billable hours and costs of investigation, remediation and restoring the systems, not to mention reputational damage and the possibility of legal action.

To ensure data security while working remotely, law firms could consider adopting the following recommendations:

- Use secure and encrypted communication channels for emails and video calls
- Use multi-factor authentication (MFA) for remote access to the law firm's systems
- Use virtual private networks (VPNs) to encrypt internet connections when accessing client information remotely
- Encrypt sensitive documents and files

(please see Appendix A for further details)

There is no one-size-fits-all and firms need to assess their existing IT set up and adopt appropriate measures to maximise data security. Practitioners are reminded that Principle 1.07 of the Guide and the commentary which makes reference to the international standard to manage IT security.

2. Proper Use of Instant Messaging Apps

The use of instant messaging apps like WeChat and WhatsApp is ubiquitous. They are convenient and allow real-time transmission of messages. However, they pose a host of security issues and risks of compromised standard of work to law firms, such as:

- **Unsecured communication**: The communications on instant messaging apps may be unencrypted and vulnerable to hacking. Law firms should avoid communicating sensitive and confidential information on instant messaging apps with clients or amongst colleagues.
- **Difficulty in record keeping**: Firms typically do not have control over the personal messaging apps of their lawyers. Unlike email, correspondence and files transferred over instant messaging apps can be deleted easily and not retrievable. Many law firms also have document management systems in place for record keeping but there is no equivalent system for instant messaging apps, making message correspondence susceptible to loss when the device is lost or stolen, or if the lawyer leaves the firm. Loss or lack of such records could be problematic for law firms if disputes later arise over instructions or communications over instant messaging apps. The absence of – or even incomplete – record of communications with clients creates challenges for the defence of professional negligence complaints or claims.
- **Unsuitable medium for workplace communication**: Instant messaging apps are designed for convenience, not as a medium for solicitors to provide legal advice. The layout and functions of messaging apps fall short of traditional email communication or letters. Communication by instant messages risk compromising the quality of solicitors' communication or advice to clients. The problem is exacerbated as there is generally an expectation that the recipient will respond immediately (e.g. a solicitor on leave or working on multiple matters might be tempted to respond immediately without making an informed decision or seeking input from his or her supervisor).
- **Lack of visibility and supervision**: Because messaging apps are usually on personal devices, the firm has no visibility over the communications with clients over this medium.

Firms should consider the following suggestions to manage the risks of using instant messaging apps:

- **Prohibit or Restrict Use of Instant Messaging Apps**: Ideally, messaging apps on personal devices for client communications should be prohibited. If communications over messaging apps are necessary, communication of sensitive information or confidential matters should not be permitted. Unless the firm has enterprise messaging platforms enabling it to control, access and

retrieve the data (with the benefit of encryption), the use of instant message apps should be kept to a minimum.

- **Regular Back-ups**: Where there has been the use of instant messaging for matters, firms should ensure that the chat history with the client is exported to firms' case management system for record keeping and to mitigate the effects of accidental deletion or loss of chat history.
- **Enhanced Mobile Device Security**: Secure mobile devices in which the instant messaging apps are installed (e.g. password or biometrics, 2FA for WhatsApp, VPN, etc). Weak security of mobile devices may result in unauthorised access to the messages exchanged in these apps.

3. **Client Identification and Verification**

According to Practice Direction P on Anti-Money Laundering and Terrorist Financing, solicitors must take reasonable measures to identify and/or verify the identity of their clients (Paragraph 104, Annexure 3 of Practice Direction P). Remote work complicates the process of client identification and verification, which is crucial for compliance with anti-money laundering regulations. In a remote work environment, solicitors may be unable to examine originals of identification or registration documents, which is the recommended practice for client identification and verification (Paragraph 105, Annexure 3 of Practice Direction P).

Practitioners are reminded of the Law Society Guidance issued in September 2022 which set outs alternative processes to verify a client's identity, including: (i) use of copies of documents certified by an acceptable identity agent such as Notary Public, Certified Public Accountant; (ii) video conferencing method; (iii) dual verification process by reviewing multiple documents from different reliable sources; (iv) third-party validation; and (v) use of "recognised digital identification system". Below are some recommended best practices for conducting client identification and verification remotely:

- **Digital Verification Tools**: Utilize digital verification tools that comply with regulatory standards. Based on Circular 23-310 (SD) dated 25 May 2023, an example of a recognised digital identification system which may be used for identity verification of a natural person is the iAM Smart platform developed by the Office of the Government Chief Information Officer. Law firms can integrate iAM Smart into their IT environment by submitting an application to the Law Society. The Circular also clarified law firms can continue to use solutions provided by the third party vendors commonly referred to as e-KYC or e-CDD for remote client on-boarding where conduct of identity verification is undertaken on the basis of a document provided by a government body i.e. HK ID card or passport, official identity document(s) issued by the Government using appropriate technology.
- **Document Inspection**: Where possible, inspect original documents via secure video calls. Solicitors should also separately request clear and legible copies of the identification or registration documents.
- **Record Keeping**: Maintain detailed records of the verification process, including screenshots and video recordings.

4. **Supervision and Training**

Law firms shall ensure their offices are supervised and managed in accordance with Cap. 159H Solicitors' Practice Rules (Principle 2.04 of the Guide). Remote work can bring about lax supervision of junior staff and non-qualified staff which leads to increased risk of negligence and wrongdoing. The law firm and the supervising partner personally will be vicariously liable and exposed to claims for professional negligence. The Law Society Circular 20-472 (SD) discussed concerns over the supervision and training of trainee solicitors during the COVID-19 pandemic. The circular helpfully provides a list of elements to be addressed in any remote supervision arrangement, such as methods of communication, frequency of contacts, management of workflow, monitor of work progress, respective obligations of the principal and the trainee, risk management strategies and record of the arrangement in addressing the above key elements.[1]

Law firms can also adopt the following strategies to ensure effective supervision and training of junior staff and non-qualified staff:

- **Regular Check-ins**: Schedule regular video calls to discuss ongoing matters, monitor the work progress of junior staff and non-qualified staff and provide guidance or feedback.
- **Mentorship Programs**: In addition to the management of workflow, the professional and personal development of junior staff may also be affected by the lack of in-person interaction with senior staff. Law firms can implement remote mentorship programs to provide extra support to junior staff.
- **Training Sessions**: Conduct virtual training sessions on key topics such as confidentiality, data security, and conflict management.
- **Systematic and Standardised Supervision**: Principals should consider putting forward guidelines or systems outlining key elements of remote supervision arrangement to ensure all junior staff and non-qualified staff in the firm are subject to an appropriate level of supervision. This includes, for instance, having oversight over correspondence and prohibiting or restricting the use of instant messaging apps. This is particularly important if remote working is permitted or common.

Conclusion & Key Takeaways

• Remote work offers flexibility and convenience, but it also presents unique ethical and legal challenges for solicitors in discharging their duty to their clients.

• It is important to have in place adequate data security measures as the consequences of theft or leakage of confidential sensitive information are drastic.

• Remote working has also resulted in more communications over instant messaging apps and there are risks associated with the use of these apps with clients. Firms need to carefully consider their approach and policies.

[1] Please note Rule 9(1) of Cap. 159J Trainee Solicitors Rules requires trainee solicitors to have their training conducted in the offices of their principals and hence remote work arrangement should not apply to them.

• There are also complexities of client identification and verification in a remote setting and these issues can be addressed through the use of digital verification tools and maintaining detailed records of the verification process.

• The lack of, or absence of, supervision or oversight by senior lawyers over their staff due to remote working is a cause of complaints and claims against firms and specific arrangements need to be put in place to ensure that firms continue to meet the high standards of professional conduct expected in the legal profession.

APPENDIX A

(a) **Use of Secure Communication Channels:** Ensure that all communications, including emails and video calls, are conducted through secure and encrypted channels.

(b) **Enable Muti-Factor Authentication (MFA)**: MFA should be implemented for all staff working remotely and requires access to the law firm's systems. MFA essentially requires users of law firms to verify their identity in two or more ways before they can gain remote access to the environment.

(c) **Virtual Private Networks (VPNs):** Use VPNs to secure internet connections when accessing client information remotely. VPNs encrypt the users' internet traffic and prevent third parties from tracking users' online activities and the data sent and received.

(d) **Data Encryption:** Encrypt sensitive documents and data stored on devices with a password. This significantly mitigates the risks of data breaches as even if unauthorised persons gain access to such encrypted information, they may not be able to decrypt it. Law firms should also ensure they have a strong password policy to ensure all encryption are effective. Enhancing password strength is not as difficult as imagined. According to the latest NIST recommendations, *password length* is a primary factor in characterising password strength (see https://pages.nist.gov/800-63-4/sp800-63b.html).

(e) **Timely Software Updates:** Install updates of software and operating system ("**Patches**") as soon as possible. Patches commonly address security vulnerabilities (e.g. zero day vulnerabilities) and thus enhance data security. Law firm staff should enable automatic software update or check for updates regularly to ensure timely instalment.

(f) **Regular Security Audits:** Conduct regular security audits to identify and mitigate potential vulnerabilities.