Scam Alert for Conveyancing Lawyers - 22 May 2019

The Law Society has received alarming information from a law practice on a scam in a conveyancing transaction which resulted in loss of monies for the client.

THE SCAM

Keeping with their usual practice, the law firm sent a letter attached to an e-mail to the client for the balance funds to be paid via purchase of a cashier's order. The law firm asked for a cashier's order in favour of the CPF board as part of the payment to the vendor. This e-mail was sent on Tuesday, 23 April 2019. The same letter was posted to the client's address. The client e-mailed the law firm acknowledging receipt. The completion date was Tuesday, 14 May 2019.

In the following days, there were e-mails exchanged between the client and the law firm on the completion date. The last e-mail from the client agreeing to purchase the cashier's order was sent from the client on Friday, 10 May 2019.

On the morning of Tuesday, 14 May 2019, the law firm called the client to ask what time he would come by to give them the cashier's order. The client was shocked to receive the phone call and informed the law firm that he had already transferred funds to a Bank of China account in Hong Kong as requested by the firm's e-mail to him. He received this e-mail informing him of a change in payment mode on Wednesday, 24 April 2019 at 3.04am. However, the law firm's server showed no such e-mail sent at the date and time.

Subsequent investigations revealed that the client's e-mail account had been hacked and the scammer had been impersonating the solicitor. The scammer had purchased a domain name that was very similar to the firm's name. For example, if the firm's name was **firstlaw.com.sg**, the scammer purchased **firstlaw-com.sg** and created several fake e-mails using this e-mail domain. The difference was a hyphen instead of a full stop. For example, if the legitimate e-mail address was '**lawyer@firstlaw.com.sg**', the scammer would use '**lawyer@firstlaw-com.sg**'. The difference between a full stop and a hyphen would go unnoticed and the client would not think twice before responding. In this particular case, the scammer went to the extent of using the secretary's name and cc-ing her in scam e-mails to the client. For example, using '**secretary@firstlaw-com.sg'** instead of '**secretary@firstlaw.com.sg'**

Once the scammer had hacked into the client's e-mail account, the scammer (impersonating as the solicitor) sent the client e-mails informing him of a change in

payment mode. The client was told to do a telegraphic transfer instead of purchasing cashier's orders.

In addition, the scammer sent to the client two different versions of the law practice's letter of completion requesting for funds. The scammer had tampered with these letters by cutting and pasting on the law practice's original letter of 23 April 2019. The first letter indicated the client should make the transfers to an account in Spain under account name CPF Board and the second letter showed a Bank of China account in Hong Kong under the name of a company. The client did not notice that both letters bore the same date. Instead, the client proceeded to ask for confirmation on which account he should transfer the funds to. He transferred funds to the Hong Kong account without informing the law firm. He transferred the funds on Monday, 6 May 2019 because the scammers had told him that the completion date would be brought forward if he transferred the funds earlier.

The law firm had no idea the client had transferred the funds via telegraphic transfer because the scammer had sent e-mails to the law firm impersonating the client by changing the e-mail slightly - for example, the erroneous '**cleint@gmail.com'** instead of the proper '**client@gmail.com**'.

Both the law practice and the client have made police reports and are waiting to hear further from the police.

LAW SOCIETY'S ADVISORY

This is a very worrying trend as it appears scammers and criminals are targeting firms which do conveyancing work and the exchange of e-mails suggests some knowledge of conveyancing practice including completion dates and keys handover. However other areas of practice that involve the transfer of funds are equally vulnerable.

The criminals are purchasing domain names very similar to the domain names of law firms to pass off as the actual law firms.

Apart from being alert and vigilant at all times, we recommend that you take the following steps to keep yourself, your law practice and your client safe:

1. Advise your client that if they receive an e-mail request purportedly from you/your firm for funds transfer/payment (by whatever mode), to verify with you/your firm first **before** effecting such payments;

2. When dealing with client demographics who are not IT savvy (e.g. some elderly clients), please take appropriate steps to clearly communicate payment instructions to them;

3. When dealing with foreign clients and permanent residents who are less familiar/unfamiliar with our conveyancing process and timelines (including payment milestones), take time to explain the same to them (preferably in writing as well); and

4. Advise your client that if they receive any instruction deviating from your last communication with them, to re-confirm with you **before** taking any action.