Case studies

Case studies

Bogus law firms

Bogus law firms

Updated 25 November 2019 (Date first published: 24 July 2015)

Print this page [#] Save as PDF [https://media.sra.org.uk/pdfcentre/?type=Id&data=992531477]

Examples below should be read in conjunction with our Risk Outlook [https://media.sra.org.uk/archive/risk/risk-outlook/]
.

Example 1

Fraudsters intercept solicitor-client emails to steal money

The following case illustrates why firms and clients should consider following up on unusual communications, using independent and established means.

Mrs A was being advised by XYZ Solicitors in the purchase of a buy-to-let property.

The day before she was due to send the purchase money to the solicitors, Mrs A emailed them to confirm details of the firm's bank account. She received two replies, both seemingly from her solicitor.

The first email contained the correct bank details. The second email, received minutes later, contained details of an account in the name of XYZ Solicitors but with a different bank. The email explained that the firm was having issues with their usual bank, and asked Mrs A to use their alternate account. This email was sent by fraudsters.

Mrs A called her bank and arranged for the funds to be transferred within 24 hours. She emailed the law firm to confirm this. This email, along with others sent by Mrs A and her solicitors, were deleted to prevent detection. The fraudsters also sent emails to both parties, assuring them everything was fine.

Three days elapsed, during which time the fraudsters transferred the money abroad.

They did this through several smaller transfers to avoid questions from their bank.

The fraud came to light only when XYZ Solicitors called Mrs A to find out what was happening. By the time the fraudsters' banking provider was alerted, all the money was gone. Mrs A's bank refused to refund her as they had acted on her instructions, leaving her to bear the loss.

It emerged that the fraudsters had hacked into the firm's email server, possibly by taking advantage of an outdated antivirus, internet browser or operating system.

They had used a bank account in the name of the law firm to make the fraud appear legitimate.

Example 2

Non-solicitor employee impersonates solicitor

The following case illustrates that fraudsters are not always faceless individuals – they can be people you know.

Mr Z was a sole practitioner in Z Solicitors, based in Bristol. He specialised in personal injury, and employed a non-solicitor to handle all administrative tasks.

We received two reports, within the space of a week, indicating that an individual was pretending to be a solicitor by using Mr Z's identity. Both reports referred to a Mr Z of Z Solicitors Ltd, based in Liverpool.

The first report was made by a member of the public after receiving a claim notification form, supposedly from Mr Z. When the individual visited the Liverpool address on the letter, he discovered the office was boarded up and had evidently not been in use for some time. We had no record of a Mr Z working from this Liverpool address. As a result, a scam alert was released on our website.

The second report was from a solicitor, after receiving correspondence from Z Solicitors Ltd. As the solicitor had never worked with Z Solicitors before, she performed due diligence checks and found the scam alert. This prompted her to make the report.

Our investigation revealed that Mr Z's administrative officer had deliberately entered false firm name and address details into several files on the case management system. She had done this to intercept payments to personal injury claimants.

We reported the administrative officer to the police for fraud and banned her from working in solicitors' firms.

Example 3

Fraudsters hijack firm's telephone line to cash fake cheques

The following case illustrates how law firms can be targeted to facilitate fraud, sometimes without their knowledge and through no fault of their own.

A law firm contacted us to report a fraud.

The firm's telephone line had been out of order on the previous Friday. When a partner of the firm dialled the number, it was answered by someone who claimed to be from their telecommunications provider. He said he was correcting a fault with the connection.

The following Monday, the firm received a call from a cheque cashing company. They advised they had called on Friday after a customer brought in two large cheques, seemingly issued by the firm. They had spoken with a Mr Z, who had said the cheques were genuine. As a result, the company had paid cash to the bearer.

The firm advised they had never heard of Mr Z, and that their telephone line was out of order at the time.

Minutes later, a client called to ask if the firm had received the money she had sent on Friday for a house purchase, after ringing to obtain their bank details. The firm had not.

The following investigations revealed the firm had been targeted by fraudsters. The fraudsters had contacted the firm's telephone company and convinced them to divert all calls to a number they were operating. They then presented fraudulent cheques in the name of the law firm. When the cheque cashing company had telephoned the firm to ask whether the cheques were genuine, the fraudsters had answered and said they were.

The fraud was reported to the police, who advised that the fraud could have been detected earlier if the firm had called their telephone company using an established number. It is not known at this stage whether the victims will be able to recover their money.

Example 4

Fraudsters hijack law firm's invoices

The following case illustrates how maintaining an up to date computer system, with antivirus software, can help protect firms against fraud.

A medium-sized law firm, XYZ Solicitors, sent invoices to nine clients by email. The firm provided details of their client bank account and asked for the payment to be made within four weeks.

Two weeks went by, but the firm failed to receive any payment. The practice manager, Mrs A, called one of the clients to make enquiries. The client said he had made the payment immediately after receiving the invoice, using the bank details provided on the invoice.

Mrs A obtained the details from the client and checked them against a bank statement. They did not match. However, the account the client had made the payment to was in the name of XYZ Law, which was similar to their own.

Mrs A subsequently called the other eight clients and found they had also paid into XYZ Law's account. When Mrs A called our Contact Centre to ask about the firm, she was told that it didn't exist.

The following investigations indicated that fraudsters had hacked into the firm's email server, intercepted the emails, and replaced the attached invoices with fraudulent ones containing different bank details. The fraudsters had deliberately used a bank account in a name similar to that of the law firm to make the fraudulent invoices appear legitimate. By the time XYZ Solicitors became aware of the fraud, the fraudsters had already transferred the money abroad.

The firm later consulted an IT security expert who advised that using an up to date antivirus, internet browser and operating system may have prevented the fraud.