DRN-3549599

Complaint

Mr and Mrs H (represented by their solicitor) complain that Excel Currencies Limited ('Excel') allowed a fraudster to transfer funds from the sale of property they owned to a bank account in Hong Kong.

For ease of reading, I will treat all submissions from Mr H, Mrs H and their representative as having come from Mr H himself. I will also refer to both Mr H and Excel's communication with the fraudster as just that; to be clear, I am not concluding that either party knew they were communicating with a fraudster.

Background

What Mr H says
In early 2018, Mr H decided to sell his holiday home in Cape Verde in order to fund a property purchase for his daughter. The holiday home was sold in May 2018 for €285,000 (€300,000 less a reservation fee of €15,000).

The agents used by Mr H in Cape Verde recommended he use a currency exchange service to receive the money in the UK in order to get the most favourable rate of exchange. They suggested that Mr H use Excel and that he contact a specific member of staff. For the purposes of this decision, I'll call that member of staff 'Mr B'.

In April 2018, Mr H sent an email from his personal email address intended for Mr B (using Mr B's Excel email address) in order to discuss instructing Excel's currency exchange services. However, a third party appears to have fraudulently intercepted this and other email communications from Mr H to Mr B from this first email all the way through until the fraud had been executed.

This enabled the fraudster to create an email address similar to Mr H's actual email address and to open an account with Excel in Mr H's name using this fake email address as well as a fake telephone number. The fraudster did this in such a way that at no point was Mr H aware that the fraudster had 'hijacked' his communications and was 'standing between' him and Mr B. So, at all material times Mr H and Mr B appear to have thought they were communicating with one another when in fact they were communicating through the fraudster, who was thus able to use information from the emails they attempted to send to one another to give directions/instructions relating to the funds Excel held which originated from the sale of Mr H's property.

Prior to receiving the funds from the property sale, it was necessary for Mr H to pay a notary fee in Cape Verde. Mr H believed he was instructing Excel to do this, though in fact the fraudster intercepted the emails where he sought to do so, and so as a matter of fact it was the fraudster who gave Excel the instructions to make this payment. Mr H made the payment to Excel in two instalments (totalling €3,756), with Excel then paying this to the notary in Cape Verde on the fraudster's instructions. The property sale funds were then received to Excel's currency cloud account at the end of May 2018 where they were held in a payment 'wallet' within the account.

On 24 April 2018, the fraudster - posing as Mr H - explained to Mr B that he and Mrs H were looking at buying a sailing boat as they were giving themselves an 'adventure' for their retirement. They asked if it was possible to change the money to USD and transfer this to the seller in China when the time comes. Mr B said this shouldn't be a problem. The fraudster contacted Mr B multiple times to chase the funds from the proceeds of the sale. On 25 May 2018 Excel confirmed to the fraudster that the proceeds from the property sale had been received. Following this confirmation, the fraudster asked Excel how much it would be if the funds were exchanged into USD. The fraudster then explained the money would be going to his brother-in-law in Hong Kong who is an agent of 'Princess Yacht'. He provided the bank details for the payment, but the beneficiary was listed as 'New Ganhon Trade Limited' not 'Princess Yacht'.

Excel's compliance team carried out a spot check on the payment. They said they thought the account would be used for a property sale and asked for further detail around why the reference indicated the purchase of a boat. They also requested an invoice and explained that it was a routine check given the size and destination of the transaction. Excel asked the fraudster for an invoice for the yacht, which the fraudster duly provided and it was sent to the compliance team, along with the fraudster's explanation of the payment instruction. The compliance team then arranged the transfer in accordance with the fraudster's instructions. On 29 June 2018, Mr H emailed Mr B to ask for the funds to be transferred to his account. Excel states that it was only at this point that it received Mr H's genuine emails from his actual email address. On Mr H's own account it appears that the fraudster had now moved on and stopped intercepting Mr H's emails. On 2 July 2018, Mr B replied to Mr H and asked if further funds had been received, as the initial funds had been sent to Hong Kong. At this point Excel and Mr H realised that a fraud had taken place.

Mr H complained to Excel and stated it acted in breach of trust by transferring the funds to Hong Kong, and that the result was that Mr H lost his life savings.

What Excel says

Excel explained it had a relationship with the agents in Cape Verde for over 10 years and the agents had advised that Mr H would be in touch to discuss exchanging funds from the sale of their property in Cape Verde. Excel says that it didn't receive any emails from Mr H's genuine email account until 29 June 2018 and that all prior emails were with the fraudster. The fraudster submitted an account sign up form using Excel's website. That appears to be Excel's preferred method of opening accounts as per the 'Becoming a client' section of its terms and conditions from January 2019 (which I understand are likely to be substantially the same as those in operation at the point Mr H attempted to open his account). Solicitors acting for Excel have previously indicated that the *'terms and conditions available on Excel Currencies' website make clear that the sign up form must either be returned in hard copy or completed online'* and that Mr H failed to do this. They argue that – had he done so – Excel would have had his correct details. However, because Mr H had attempted to send scanned copies of the hard copy documents by email the fraudster had been able to do so, accompanied by copies of Mr and Mrs H's address and identification documents.

The fraudster intercepted Mr H's email and submitted the relevant information using one of the approved methods. This included a phone number, purporting to be that of Mr H, but which was in fact a different number. Excel conducted a 'Smartsearch' check using Mr and Mrs H's personal details to verify their identity. When both checks passed, Excel activated the account in their name.

Excel stated that when the fraudster requested that the funds were sent to Hong Kong, it followed its correct processes, including obtaining an invoice for the purchase of the yacht. On 2 July 2018, Excel began investigating this matter. The investigation included whether

there was an irregularity on Mr B's part. It concluded that there was no evidence that Mr B was involved.

Excel also worked with Microsoft to conduct an email message trace, recover deleted data, analyse IP addresses and investigate logon activity for Mr B. The Microsoft team did not recover any emails sent from Mr H's genuine email address, nor did it send emails to Mr H's genuine email address. Excel says that it noted that the IP addresses associated with the fraudulent emails were sent from IP addresses in Poland and Nigeria and it concluded that the third party appears to have intercepted emails sent by Mr H and responded to him purporting to act of Excel.

Excel reported the matter to Action Fraud.

On 14 January 2022, I issued a provisional decision upholding this complaint. For completeness, I repeat my provisional findings (which form part of this final decision) below:

I have considered all the evidence and arguments to decide what is fair and reasonable in all the circumstances of this complaint.

I've first considered whether the Ombudsman Service has jurisdiction to consider the complaint.

When the Hong Kong payment took place, Excel was a registered small payment institution. Under DISP 2.3.2A the Ombudsman Service can therefore consider a complaint under the compulsory jurisdiction, provided that (i) Excel was carrying out 'a relevant activity' (or 'ancillary activities' in connection with them), (ii) H is an eligible complainant, (iii) the complaint is within time, and (iv) there are no territorial issues taking it outside of jurisdiction. I'm satisfied that Excel was carrying out a 'relevant activity'. The complaint relates to Excel's acts/omissions in carrying on a payment service - in this case that was the execution of payment transactions. It also relates to ancillary activities carried on in connection with that service – in this case, that was creating a customer account and receiving and holding funds in that account to be used in those payment transactions.

I've then considered whether Mr H is an eligible complainant. He's a consumer, because he is a natural person acting for purposes outside a trade or profession. He therefore comes within DISP 2.7.3R(1).

I've gone on to decide if Mr H falls under any of the eligible complainant relationships in DISP 2.7.6R. I don't think Mr H was a customer or payment service user of Excel, so he isn't eligible under 2.7.6R(1). That's because, although Excel opened and held an account in Mr H's name, it never dealt directly with Mr H - the fraudster sent all of the paperwork to open the account, operated the account and issued the order for the Hong Kong payment. Therefore there wasn't a valid contract between them, because the fraudster didn't have any legal authority to act on Mr H's behalf. Where a person opens an account in the name of another person without any authority so to do, there is no customer relationship. And Mr H can't now ratify or validate the fraudster's actions in opening the account in his name. However, I think that Mr H <u>was</u> a potential customer/payment service user of Excel. He's therefore an eligible complainant under 2.7.6R(2). I've decided this because both Mr H and Excel both intended for Mr H to be a customer, and both actively took steps towards making this happen. Excel attempted to send its account opening documentation to Mr H and – although it was intercepted - Mr H completed and tried to send that documentation back to Excel. Both believed that Mr H had properly opened an account, even though the fraudster's actions meant that there wasn't a legal relationship between them. They both took steps in relation to two smaller transactions prior to the Hong Kong payment, and both of those transactions went through successfully. It was only the fraudster's actions that prevented a

formal legal relationship between Mr H and Excel, and both of them acted in a way consistent with Mr H being treated as Excel's customer. I think that's sufficient for Mr H to be a potential customer or payment service user for the purposes of DISP 2.7.6(2).

Although I'm already satisfied that Mr H is an eligible complainant for the reasons I've given above, I've also considered whether Mr H had a relationship with Excel where he was beneficiary under a trust where Excel was trustee (DISP 2.7.6R(13)). This is because, in his complaint to Excel, Mr H also suggested that Excel had acted in breach of trust. Excel's Terms & Conditions show that Excel intended - and thought it had agreed with Mr H - to hold money in a separate client account for him as the ostensible account-party. I think that would be sufficient for there to be an express trust between them if there was a valid contract between them, which would mean Mr H was eligible to complain to us in his capacity as a beneficiary under a trust. However, because of the fraudster's actions in intercepting the communications between Mr H and Excel, there was no contract between them. I think that in this case a contract was necessary for there to be a trust, and that DISP 2.7.6R(13) only applies to such 'express' trusts. The fraudster had no authority to act on Mr H's behalf, to make a contract, or to deal with Mr H's property. There was therefore no contract between them, and no trust.

The complaint was raised with Excel and referred to us within the necessary time limits, so we are able to consider it.

Because Excel made the Hong Kong payment from an establishment in the UK, Mr H's complaint comes within our territorial jurisdiction.

Having decided that the complaint is within the Ombudsman Service's jurisdiction, I've now gone on to decide what's fair and reasonable in the circumstances of the case. In particular, I've considered (i) issues relating to the account opening, and (ii) issues relating to the transfer of funds.

Account opening

I reviewed email correspondence between Mr H's agent in Cape Verde and Mr B. In an email from the agent to Mr B dated 19 April 2018, the agent states:

'I'm trying to get (Mr H) to use you. I gave your details. We just sold their villa in Sal for €300k…Hopefully he will contact you. Will be transferring about €285k back to sterling when it happens hopefully.'

This email was sent prior to Mr H contacting Mr B. I therefore think it was the understanding of all parties involved (from the outset), that Mr H intended to use Excel as a currency exchange service to receive and exchange proceeds from his house sale, with Mr H ultimately receiving the money.

We requested Microsoft's findings (which Excel relied upon to conclude Mr H's email account was the likely cause of the 'hack'). Excel could not provide this information as it stated it did not receive a report at the time of Microsoft's investigation. When it requested a report following our involvement, Microsoft advised that no internal notes were recorded, no logs could be pulled and the person that worked on the case no longer worked for Microsoft. I do find it peculiar that Excel did not insist upon a report from Microsoft at the time it investigated this matter given the scale of the loss and the allegations made against it by Mr H. If no report was created and it kept no record of Microsoft's findings, I'm unclear as to how it was able to recall Microsoft's findings in a letter to our service almost a year after instructing Microsoft and keeping no record of its findings.

Mr H on the other hand has produced evidence that he emailed Mr B from two separate email accounts (his personal and his business email addresses) and provided evidence that both accounts were held on separate servers. I asked Excel if it had received emails from either account and it advised it had not. I've noted:

1. *Mr B was advised to expect Mr H's contact (by email), from a long-standing relationship Excel held with his agents in Cape Verde and this email explained what the nature of the contact would be.*
2. *The email from the Cape Verde agents to Mr B outlined the details of the buyers of Mr H's property. I've noted the fraudster shared this information with Mr H in later correspondence and this is not something Mr H shared directly with Mr B for the fraudster to have known.*
3. *Mr H never had prior dealings with Excel and was given specific contact details of Mr B by the Cape Verde agents.*
4. *The fraudster created a new email address for Mr H (very similar to his actual email address), which it always communicated with Mr B on. If the fraudster had control of all Mr H's email accounts, it's unlikely the fraudster would have needed to take steps to create a new email address to communicate with Mr B as Mr H.*
5. *Mr H appeared to receive emails from Mr B's genuine email address to his genuine email account.*
6. *Mr H emailed Excel from two separate email accounts, held on different servers, and neither email was received by Excel.*
7. *Excel stated that Microsoft provided no report when it investigated this matter and kept no record of the contact that was made which allegedly pointed to Mr H being the victim of an email intercept scam.*

The common thread in Excel's introduction to Mr H by the agents in Cape Verde and Mr H's introduction to Excel by the same agents is Mr B's email account. I don't find it plausible that an unknown fraudster had access to two of Mr H's separate email accounts (held on separate servers) sufficient to have known when he would email Mr B so that those emails could be intercepted. I've also drawn inferences from Excel's failure to produce material evidence regarding Microsoft's findings.

I find it more likely than not that Excel's email systems were hacked by a fraudster. Another option is that Excel were complicit in the fraud. However, on the basis of the evidence available and likely to become available this is no more than speculation, so I cannot be satisfied on the balance of probabilities that Excel was complicit in the fraud.

I've also taken into account the submission put forward on Excel's behalf that Mr H tried to open his account by emailing the forms to Excel, and that this was not one of the approved ways of opening an Excel account. And I note that, having intercepted the email and attachments (namely the account opening paperwork and identity documents) the fraudster did not send that paperwork on by email, but rather opened the account in Mr H's name using Excel's online portal.

Notwithstanding what Excel has said, I note that the January 2019 terms and conditions I referred to above say that, in addition to sending in hard copies or using the online form 'An alternative to signing our trading agreement, is to send in the electronic documents required to activate your account.' This appears to me to be what Mr H attempted to do, but the fraudster intercepted that email. So I'm not persuaded that Mr H necessarily used an unapproved process when he tried to open the account.

*The FCA defines Firms' responsibilities in the Principles for Businesses. Principle 2 requires that 'a firm must conduct its business with due skill, care and diligence' and Principle 3 that 'a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems'. The FCA's Financial Crime Guide (**FCG**) underlines firms' responsibilities in respect of preventing financial crime, which includes a section on data security. In addition, regulation 98 of the Payment Services Regulations 2017 (PSRs) requires that payment service providers such as Excel establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services it provides.*

In light of the above, I think it's clear that the integrity of Excel's email systems were of fundamental importance in how it runs its business. As I said above, I'm satisfied that its more likely than not that the reason the fraudster was able to hijack Mr H's correspondence is because the fraudster hacked Excel's systems. I think that is sufficient to support the conclusion that Excel did not have adequate security in place. And I note that Excel haven't provided any reliable evidence that would rebut this. So I think it's fair to say that Excel's systems weren't adequately secure, and that this enabled the fraudster to hijack Mr H's correspondence, open the account in his name, and carry out the fraud.

Even if I am wrong that Mr H tried to open his account in a way provided for by Excel's terms and conditions, I am satisfied that email security was of such fundamental importance that the failures I've identified are sufficient to uphold the complaint. First, I am not aware of anything in the terms and conditions or elsewhere that warns customers against corresponding with Excel by email, or that indicates that email represents a significant risk over and above other forms of correspondence/account opening. Second, Excel was obviously content to correspond with clients and potential clients, including in respect of account opening and prior to the account being opened. Excel routinely corresponded with the fraudster (posing as Mr H) by email for around two months, illustrating the extent to which email is an important part of its everyday business. Finally, I think it is reasonable to conclude that if another customer had sent scanned copies of their paperwork as Mr H did, Excel would have opened an account for them as though they had sent hard copy documents. I've considered whether the way in which Mr H tried to open the account might suggest that any award should be reduced on the basis of what's known as contributory negligence. However, for the reasons set out above, I don't think it should. I'm satisfied that it was not essential for him either to use the online submission or send hard copies to open his account with Excel, and I consider the fact that the fraudster was able to hijack all of his correspondence with Excel (which includes emails he sent prior to sending the account opening paperwork) was the root cause of the fraud taking place.

So on that basis, I uphold the complaint. But because of the arguments raised on Mr H's behalf, I have gone on to consider whether Excel should have done something to try to prevent the eventual transfer of funds.

The transfer of funds

I think it is helpful to set out both Mr H and Excel's intentions in regards to Mr H's property sale proceeds:

On 23 April 2018, after a conversation with Mr H's solicitors in Cape Verde, Mr B wrote to the fraudster and recommended the following steps to facilitate the transfer of funds:

1. *The buyers of Mr H's property in Cape Verde would send the Euros to Mr H's lawyer*
2. *The lawyer would send the Euros to Excel's Euro account in London*
3. *Excel would exchange the Euros into sterling and send it to Mr H's sterling account*

Steps one and two were followed. But step three was not. This is because the fraudster wrote to Mr B and – a change from what Excel understood to be the original plan - advised that Mr H wanted to purchase a sailing boat from Hong Kong for he and Mrs H to take an 'adventure' for their retirement.

I've reviewed the account's terms and conditions to see how it was agreed for the payments to be made. These say to make a trade, Excel may accept written or verbal instructions and these written instructions can include an email. The terms also say that each trade request would form a separate contract for services between Excel and its customer. Excel says it will make trades in good faith and is under no duty to challenge or make enquiries concerning written instructions it genuinely believes to originate from its customer's wishes. And finally, it may at its discretion refuse any trade without giving reasons.

I accept that Excel's processes allow it to accept payment instructions by email. But in doing so, it must accept that fraudsters can infiltrate such systems. It didn't have any additional security or payment authentication processes at the time. So I've considered whether I think it ought to have done more.

In broad terms, the starting position at law is that a payment service provider such as Excel is expected to process payments and withdrawals that a customer authorises it to make. That was the case in May/June 2018, and remains so now, and I have taken this into account when deciding what is fair and reasonable in this case. Although I accept that Mr H was not its customer as a matter of law, given that (i) both Excel and Mr H intended for him to be a customer, and (ii) Excel believed that he was a customer, I consider that it is fair and reasonable to look at the complaint based on how Excel was required to treat customers. Taking into account the law, regulatory rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Excel should fairly and reasonably:

- *Have been monitoring accounts—and any payments made or received—to counter various risks, including anti-money-laundering, countering the financing of terrorism, and preventing fraud and scams;*
- *Have had systems in place to look out for unusual transactions or other signs that might indicate its customers were at risk of fraud (amongst other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer; and*
- *In some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.*

I am satisfied there were enough 'triggers' in this case to have alerted a responsible regulated firm such as Excel that Mr H's account was being subjected to unusual and uncharacteristic activity. This is because:

- *It's unlikely that a couple based in the UK would seek Excel for a better exchange rate to facilitate the exchange of funds in Euros to £sterling, only to then convert those funds to a less favourable rate in USD to purchase a yacht from China.*
- *The funds for the yacht weren't to the selling company.*
- *The fraudster initially suggested that the seller was based in China, the invoice also confirmed this, but the payment details were made to a company based in Hong Kong.*

- *This was a significant sum of money to receive a change of instructions for.*
- *It is unlikely Mr H would have chased for updates around when the purchase monies would be received when he knew what the completion date was.*
- *The fraudster also failed to provide documents when requested.*

In my view, there were reasonable grounds to suspect a fraud or scam, and therefore justify an intervention (such as phoning Mr H in order to ask discreet questions about the nature and purpose of the payments, and to request a receipt).

Excel understood that it was being used to obtain a favourable exchange rate to transfer funds to a UK based account following the proceeds of a property sale. I think the email request to convert the property sale funds to USD and subsequently send those funds to China to purchase a yacht was sufficiently unusual to warrant further checks by Excel. It's clear there were fraud triggers based on the nature of the transaction, however the triggers came from the compliance team acting on behalf of the currency cloud to facilitate the payment transfer and the compliance team relied on Excel's responses to its queries – which it obtained via emails with the fraudster. I do think it would have been reasonable for Excel to have paused the payment instruction and properly question Mr H before processing the payment in order to satisfy itself that all was well. This is particularly so given the risk of email interception fraud and the fact that Mr H had only communicated with Excel via email. There is no evidence that Excel provided Mr H with any meaningful warnings or gave him other reasons to doubt the legitimacy of the payment he was making.

Even so, I have to consider what the impact of this was. If Excel had called Mr H and asked for more details around the payment instruction, what the payments were for and the basic surrounding context, it is likely it would have made no difference to the payment instruction. This is because it was the fraudster that opened the account, not Mr H. And upon opening the account, the fraudster provided a telephone number that did not belong to Mr H. So it's likely that Excel would have spoken to the fraudster to ask further questions. The fraudster already had Mr H's personal sensitive data, so it would have been able to sufficiently answer questions put to them by Excel.

I've noted that Excel did have conversations with the fraudster and it didn't suspect anything untoward. Whilst I appreciate the magnitude of the loss to Mr H and there are points where I accept Excel ought to have done things differently, I don't think an intervention by Excel on the basis of the transaction being unusual would have made a difference to Mr H's loss.

Responses to my provisional decision

Mr H responded to my provisional decision and queried the following:

- The sum on which Excel should pay interest.
- The exact date Excel should pay interest from.
- Whether his legal costs can be recovered or not. Mr H believes that Excel should pay his legal costs as this was a very complex matter that has required the involvement of professional advisers as he and Mrs H are elderly individuals who have found this whole experience incredibly stressful which has resulted in financial hardship for them. They've been forced to use this service to gain the compensation they deserve through initially obstructing their requests for basic information. At the time of Mr H's response, his legal costs are £9,606 plus VAT.

Excel provided a response to my provisional decision which I've read in its entirety. I've grouped together and summarised its key points below:

Account opening

- Mr H acted recklessly by failing to call the telephone number on Excel's website during the three months of his communication with the scammer, including when the scammer posing as Mr B promised huge speculative returns on his money.

Terms of business

- I have cherry picked from its terms of business.
- Its terms of business requiring hard copies of a paper form in the post are clear; Mr H clearly read its terms of business and is therefore complicit in what led to this happening.
- The alternative option to signing a trading agreement is available for online traders. They send via email their required ID only. Signing the trading agreement is clear, you send the hard copy in the post if you plan to sign it via this method. Once that person is then online and at the time of their first trade this is when they must accept the terms and conditions. This is explained in its terms and conditions.

Mr H's conduct

- I've not discussed negligence on the part of Mr H.
- The funds were received from a 3rd party in Germany not from an account held in Mr H's name or his solicitor. This was negligence on Mr H's part that contributed to him being defrauded.
- There must have been a reason that Mr H chose to avoid having funds routed through the solicitor or his own account. It may have been to avoid paying the property taxes due had the funds been sent from Cape Verde. It expected the payment from a lawyer.

Point of compromise

- Excel assisted Mr H by getting him to check his email addresses on a website which showed they were compromised. Excel asked Mr H if he ever changes his passwords and he confirmed he had not. It would be easy for a fraudster to connect the use of Mr H's two email accounts — both of which had been compromised — that had the same level of security.
- The Cape Verde agent and Mr H were in constant dialogue regarding the sale of the property and also the prospective buyer. With Mr H's emails being compromised it would be clear to the fraudster who the buyers were. Excel appear to suggest that this gave the fraudster another opportunity to target Mr H and feeds into a plausible/more likely explanation for how Mr H's emails were intercepted than that Excel's systems were hacked.
- It was easier for the fraudster to maneuver by setting up a separate email account for Mr H because if it operated solely out of Mr H's email account, it would have taken too much attention. It's more plausible that Mr H's email account was the source of the hack and it seems we are only making plausible cases for one side and ignoring the clear possibilities on the opposite side.
- The emails from Excel were not genuine and were 'spoofed' as they include UK phone numbers that do not belong to Excel.
- I have given no consideration as to why this appears to have been an isolated incident affecting only one of Excel's clients. If Excel's email systems were compromised in the way that I have suggested then this would have happened with multiple clients leading to multiple complaints.

- There is no evidence that shows Excel's email accounts were compromised – the Microsoft report would have made this 'abundantly clear'.

Microsoft report

- It requested a report from Microsoft and explained why this report couldn't be provided. The Microsoft investigator used an email analysis that could determine the IP address of the emails that were being sent by Mr H. Microsoft has since deleted the report. Excel cannot be blamed for the fact that the Microsoft report is no longer available.
- The findings and steps Microsoft took were documented by Excel's lawyers in correspondence I have seen. The statement of what took place was documented multiple times over the year. Excel had constant meetings to discuss steps taken. Had it have known what Microsoft's policies were on deleting records, it would have asked for a detailed report. Essentially, Excel's recollection of Microsoft's conclusions are reliable.
- Microsoft concluded there were no trace of any emails which was its expert opinion.

Payment instruction

- The fraudster said the yacht payment was going to an agent of Princess Yacht, rather than Princess Yacht itself, suggesting that there was nothing inherently suspicious in the invoice not being in Princess Yacht's name. And the payment passed compliance checks by its banking provider.
- The fraudster posing as Mr H changed the instructions to send the funds to China less than 24hrs after registration, and a month before it made the payment. The instructions did not change during that period.
- Its payments systems and security checking on payments are robust and it nor its payment systems providers failed to class the payment as suspicious. Excel believes that I am saying that it ought to have held the payment on 25 May 2018 and refused to action it until such time that the real Mr H uncovered the scam five weeks later. That cannot be right.
- It has clients who sell properties in various countries and use funds for other reasons than moving them back to their home country. The USD exchange rate has no relevance. The funds were sent to a broker handling the sale, and Hong Kong is part of China such that there was no reason for Excel to distinguish between the two in terms of the invoice address.
- In fact, the payment was paused and remained unsent for several days while Excel made appropriate enquiries.
- Although it accepts email requests, it has a security process which includes speaking to the client to confirm the legitimacy of their email. It does not matter what a referring partner tells Excel a client will do with their money. Excel followed this process.

Additional points

- The email from the Cape Verde agent outlining what Mr H wanted to do with the proceeds of sale has been taken out of context. Excel receives emails like this all the time from agents it partners with. Some clients contact Excel with completely different plans for what they intend to do with funds. Excel says *'It is not a certainty that can be attained that the funds would only be going to Mr H's account.'* By this I understand it to mean that there was nothing inherently suspicious about the change in instructions whereby the fraudster told Excel that the money was to be used to buy a yacht.

- Either Mr H or Mr H's lawyers in Cape Verde told the German buyer of their property to not send the funds to Cape Verde. This means that the German Buyer has never paid for the property as the funds never reached Mr H as they should have, in Mr H's Cape Verde bank account or with the solicitors acting upon the sale.
- Excel expects that I take a fair approach to what has happened and weigh up all of the events that took place.

I queried Mr H's email being compromised with him along with the conversation he had with Excel about this. I also queried the payment journey of the funds with Mr H and why they did not come from his lawyers in Cape Verde.

Mr H said in summary:

- He nor Mrs H recall being advised by anyone at Excel to check their email accounts to ascertain whether they had been compromised. Mr H confirmed he spoke to Excel and was advised to change the passwords to his email accounts. However, Mr H denies that he ever said to Excel that he never changed his passwords to his email accounts. In fact, Mr H can confirm that he did change the passwords to his email accounts.
- If Excel are seeking to rely on a particular website to track email accounts being compromised, Mr H carried out checks on this website. He noted if you type an email address in the search function, it tells you whether that email address has been subject to a 'data breach' or a 'paste'. It gives no further information as to the nature of what has happened. It noted that Mr H's email accounts was subject to two data breaches and his work email address was subject to one. However, he noted that Mr B's email address was subject to three breaches and Excel's general email address was involved in five breaches using the same website check.
- During a meeting in Cape Verde in February/March 2018, it was recommended to Mr and Mrs H by their lawyer that the sale funds should be paid directly to Excel from the Purchasers as it would be quicker and would avoid charges. And so, Mr H followed his lawyer's recommendation.

An email from Mr H's lawyers was provided explaining that when payment of the purchase price is sent to its client account, by the client's own choice, the same is transferred to the counter party on/after the completion date. The lawyer believes that some of the clients who opt to pay/receive the funds directly from the counter party, do so to avoid delays, bank charges and international transfer commission and fees from the respective banks, not an avoidance of tax.

I provided Mr H's commentary on the use of the specific website used to check his email account to Excel. It replied with recalling the call it had with Mr H:

> *'…..In this call I asked about their email accounts:*
> *What type of password do you have?*
> *Is it a word or phrase?*
> *Mr H confirmed the password used on his emails was family related.*
> *I said that I checked on I have been pwned and could see that there was breaches, what type of data was compromised and that they should change it immediately.*
> *I suggested to change them to a random mix of characters.*
> *I gave them the website so that they could check themselves.*
> *Mr H confirmed to me that he had the same password on all his email accounts and had never changed it before.'*

Excel recalled emailing Mr H on 5 July 2018 to suggest that he changes his router/WIFI password regularly too. It further noted that its team have notifications set up to alert it if its email addresses and passwords are found online.

Its general email address is an email address only – not an active email account user and it had password policies in place then and do now. Excel further noted that Mr H never changed his password, the password was related to family and was not a random mix of characters and Mr H never even considered the risks. Excel stated that Mr H's data was hacked in 2016 and 2017 and then sold on the dark web in batches. It explained many fraudsters buy the data with the sole aim of accessing email accounts to look for opportunities to obtain credit card information, intercept bank transfers, send emails to this persons contacts requesting money to be sent to a bank account.

It provided evidence that the detail of the data breaches included a breach in October 2016 and August 2017 where personal sensitive data of Mr H was obtained.

My findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having done so, I am satisfied that I should uphold this complaint and I'll explain why.

Firstly, I don't think that Mr H acted negligently in failing to recognise that he was the victim of a scam. His agents recommended Excel (Mr B at Excel specifically), and he attempted to correspond with Mr B's genuine email address. He also received emails from what appeared to be the genuine email address of Mr B. I therefore don't think that Mr H acting on the instructions of who he reasonably believed to be Mr B, representing Excel, to be unreasonable. I have taken Excel's point that Mr H was offered speculative returns on his money - by the fraudster posing as Mr B after the account had been opened around the time the payment was being processed by Excel to the fraudster - but I've also noted that Mr H declined this offer and I don't think he could have reasonably suspected this wasn't a genuine offer, or was sufficiently suspicious that it should have alerted him to the fact that he was being defrauded.

I'm further persuaded that Mr H acted on the instruction of his lawyer to receive the funds from the Purchaser directly. Having reviewed his lawyer's email, I think Mr H was given options on receiving payment and chose the one that incurred fewer charges. I do not think this was unreasonable, nor do I think that this was a material factor that caused the loss as I'm still satisfied the loss was caused as a result of Excel's systems likely being hacked. Where the sale proceeds were sent to Excel from does not appear material to how the fraudster was able to carry out the fraud, and I do not agree with Excel's suggestion — unsupported by any further explanation — that *'this negligence also contributed to what happened'*.

I've noted Excel's argument that its lawyers documented the events with it over the course of a year and it was not relying on its recollection in relation to the Microsoft investigation. But I find it unusual that neither Excel nor its lawyers would keep a record of contact notes or a report from Microsoft during the course of that year. Excel is seeking to rely on Microsoft's findings absolving it from any hacking and can provide no evidence to corroborate Microsoft's findings, so I don't find what it recollects Microsoft told it to be persuasive as it is not substantiated in any way. I have to decide the case based on the available evidence and to decide what I think is most likely. Without such a report, or other compelling evidence to the contrary, I am satisfied that it is more likely than not, on the balance of probabilities, that

Excel's systems were hacked, rather than the fraud taking place for the reasons Excel has suggested.

I further accept that Excel works with many agents and would receive emails offering it business. But the email Mr B received from Mr H's agent was specific. And therefore when Mr H did get in touch with Mr B within days of this email, it wasn't a surprise to him as he was expecting to hear from him. I made no conclusion that Mr H *would* use Excel as a matter of certainty, rather that it was all parties' (Mr B, Mr H and the agents) understanding that this was the intention.

Excel has not persuaded me that Mr H's email accounts were the likely source of the hack and I've thought about this very carefully. By Excel's explanation, a fraudster obtained Mr H's personal details in 2016 and 2017 from separate servers, was able to link the two, and waited until he decided to sell a property in 2018 to use a currency exchange service via email (so that it could be intercepted) before creating a fake email account to carry out the fraud, whilst monitoring both of Mr H's genuine email accounts. I've also noted that Mr B's email account was involved in one of the same data breaches in 2017 highlighted by Excel about Mr H's email account, so I'm not persuaded that this information is conclusive as to the outcome.

In all the circumstances I think the evidence points to Mr B's email account being compromised rather than both of Mr H's email accounts being hacked from data breaches that occurred more than a year prior to the fraud. And I am satisfied that Excel's account of how the hacking took place is somewhat speculative.

I find Mr H's testimony to be persuasive that he did have a discussion with Excel about his passwords and was advised to change them. I also find his explanation plausible that he had changed his passwords sometime prior to the fraud taking place.

I've also noted Excel's suggestion that it couldn't have been the cause of the 'hack' as this would have happened to multiple customers and resulted in complaints. I haven't concluded that Excel's entire systems were compromised but I do think (on balance) that Mr B's email account was compromised, however that may have happened. Excel has provided no evidence to demonstrate whether similar issues have been reported to it at the period of time Mr H fell victim to this scam.

Although there are reasons why it might be thought that any hack might potentially have had more widespread consequences, I am not satisfied that this possibility outweighs my main conclusion that the evidence points away from Mr H's separate and distinct email addresses being hacked in the way Excel appears to suggest. And I am satisfied that – regardless of why the fraudster chose to hack Excel's systems, whether it only hacked Mr B's accounts rather than Excel's systems more widely, and whether anyone else was involved – the key feature that led to Mr H losing his money was the fact that the fraudster was able to hack Excel's systems.

In relation to Excel's terms and conditions, I've not cherry-picked sections as it has suggested. I've referred to the opening section of 'being a client' and quoted sections that are relevant to opening an account with Excel. I've included the full section referenced by Excel in its response here for transparency:

> *'An alternative to signing our trading agreement, is to send in the electronic documents required to activate your account. You will then be given access to your online account and at the point of trading you will be given the option to agree to our terms of business, at this point and going forwards, whether you trade online or offline you will be bound by our terms of business.'*

The terms do not reference account opening for online traders only as Excel suggests, and specifically references trading online or offline with either account opening option. The fundamental point here is customers are not required to provide hard copies of paperwork as the only way of opening an account; electronic documents can be sent as an alternative – which I've noted Mr H attempted to do. Whilst Excel pointed out the forms sent to Mr H by the fraudster had been doctored, Excel's approved questions for account opening were still included on the doctored forms, the difference is Mr H returned the form to the fraudster electronically and the fraudster used this information to open the account on Excel's website. So, I make the same point that Mr H wasn't using an unapproved way of attempting to open an account with Excel.

I remain satisfied that the request to send the funds to China to purchase a yacht was unusual for the reasons I've already explained in my provisional decision. Excel has highlighted further concerns it had in its response to my provisional decision as it stated it hadn't received the funds in the way it expected yet didn't find this concerning at the point it received the funds. I explained in my provisional decision that if Excel had carried out further checks (as I believe it should have) it would have made no difference to the payment instruction. That's because it had the contact details of the fraudster and the fraudster would have likely satisfied any questions or concerns raised by Excel. So I agree with Excel that it wouldn't have been able to stop the payment if it had appropriately intervened at the time of it. But as I've explained, that is not the basis on which I have upheld the complaint.

The reason I uphold this complaint is I'm satisfied, based on all the evidence I've seen and the balance of probabilities that Excel's systems, specifically Mr B's email account, was the likely cause of the hack. And this was central to Mr H's losses. Because of this, I am satisfied that Excel should return Mr H's losses up to our award limit.

In relation to Mr H's legal costs, I have taken on board the complexities of the case and the matters involved. I also appreciate why Mr H would have appointed a solicitor given the loss at stake. However, we offer a free service and Mr H was not *required* to appoint a solicitor to represent him in using this service. My decision is not based on the strength of Mr H or Excel's legal representations, it's based on what I think was most likely to have happened in the circumstances of this complaint. And whilst I appreciate it's come at an expense to Mr H, I am satisfied that it wouldn't be appropriate to direct that Excel pay his solicitor's costs. He must therefore bear his own solicitor's fees in relation to bringing his complaint to this service.

Redress

Where I intend to uphold a complaint, I can award fair compensation to be paid by a financial business up to £150,000, plus any interest and/or costs/ interest on costs that I think are appropriate. If I think fair compensation is more than £150,000, I may recommend that the business pays the balance.

My final decision

Determination and award: For the reasons set out above, I uphold this complaint. Excel Currencies Limited should refund to Mr and Mrs H all of their stolen payment, up to our maximum award limit of £150,000.

Excel should add interest to the sum of £150,000 (less any tax properly deductible) at 8% simple per year, from the date of the loss (25 May 2018) to the date of refund. For the avoidance of doubt (in case it becomes relevant), our statutory cap of £150,000 does not

include interest or costs, which can be awarded over and above that sum (see DISP 3.7 of the *Financial Conduct Authority Handbook* for more information about our awards).

Recommendation: As the total amount of Mr and Mrs H's loss is more than our limit of £150,000, I recommend that Excel Currencies Limited pays Mr and Mrs H the remaining balance of their loss of €285,000 – also with interest at the same rate and for the same period. As proceeds of the property sale were received in Euros to be converted into £ sterling, for the avoidance of doubt, Excel Currencies Limited should apply the conversion rate Mr and Mrs H would have obtained at the time they instructed its services.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H and Mrs H to accept or reject my decision before 15 July 2022.

Dolores Njemanze
Ombudsman