Ombudsman Decision
CIFO Reference Number: 18-000424
Complainant: [The complainant]
Respondent: Lloyds Bank Corporate Markets plc, trading as LloydsBank International (Guernsey branch)

It is the policy of the Channel Islands Financial Ombudsman (CIFO) not to name or identify complainants in any published documents. Any copy of this decision made available in any way to any person other than the complainant or the respondent must not include the identity of the complainant or any information that might reveal their identity.[1]

A decision shall constitute an Ombudsman Determination under our law.

Complaint

[The complainant] complains, in summary, that Lloyds Bank Corporate Markets plc, trading as Lloyds Bank International (Guernsey branch), failed to take adequate and/or appropriate steps to ensure that a payment [the complainant] had asked it to make was transferred to the correct beneficiary.

Preliminary Matter

In my earlier Provisional Decision on this complaint I said that it had been made about Lloyds Bank (International Services) Limited. There have, however, been a number of changes to the corporate and legal structure of the bank in the Channel Islands in recent years – including since the events [the complainant] complains about occurred. Lloyds has recently confirmed to me that the bank's current legal entity is as set out at the top of this Final Decision, and that this entity has liability for relevant predecessor entities. For ease, however, I simply refer to the bank as 'Lloyds' in the main body of this document.

Background and Provisional Decision

I previously set out the background to this complaint in my Provisional Decision dated 13 May 2020 – a copy of which is attached, and forms part of my Final Decision.

[1] Financial Services Ombudsman (Jersey) Law 2014 Article 16(11) and Financial Services Ombudsman(Bailiwick of Guernsey) Law 2014 Section 16(10)

The outline background is that [the complainant] approached an investment services company, [redacted for anonymisation purposes], for advice. Their investment adviser, [redacted for anonymisation purposes], recommended [the complainant] invest in [redacted for anonymisation purposes] funds. As a result, on 18 September 2018 [the complainant] asked Lloyds to pay £434,000 from her account to [the fund]. She initially emailed the bank, to which she attached the information she'd received from [the investment services company] about [the fund's] bank account at [Bank A]. But a little over an hour later, [the complainant] sent a further email to Lloyds – in which she said the 'transfer details' had changed. [The complainant] attached an updated note [the complainant] had (apparently) received from [the investment adviser], which said the payment should be made to [the fund's] account with [Bank B].

Lloyds requires payments such as these to be instructed and authorised in person, and [the complainant] visited the bank's Smith Street, Guernsey branch on 19 September 2018 to do so. The authority was completed using the updated account details for [the fund], and the bank made the payment from [the complainant's] account.

Six days later, on the morning of 25 September 2018, the bank received an email from [the complainant] saying the money had not arrived. Later that morning, [the investment services company's] Money Laundering Reporting Officer visited the bank and said they believed [the complainant's] email account had been 'hacked'. [The investment services company] had *not* provided [the complainant] with updated bank details for the transfer. Lloyds subsequently completed an 'Authorised Push Payment Scam Notification Form', which it sent to [Bank B], and it asked for the money to be returned. However, [Bank B] was unable to recover the full £434,000. Between November 2018 and February 2019 [Bank B] returned a total of £269,886.14 to Lloyds, leaving £164,113.86 outstanding.

By way of my Provisional Decision I concluded, in summary, that Lloyds should have recognised the underlying 'email intercept' fraud risk in this case and raised that possibility with [the complainant] before the payment was made. If it had done so, I considered that the imminent fraud would quickly have come to light and [the complainant] would not be out-of-pocket in the way she is today. I therefore recommended that Lloyds should reimburse [the complainant] for the money the bank was unable to recover from [Bank B], plus interest.

[The complainant] accepted my Provisional Decision, but Lloyds did not. Over the past few months I have had a detailed exchange of correspondence with the bank, which has included some phone conversations. The bank also asked that the underlying issues be raised with the Guernsey Financial Services Commission (GFSC), and we have since had a discussion with them.

Lloyds said, in summary:

- It does not consider that the type of fraud which occurred in this case was all that well known either in the UK or in Guernsey in 2018. Moreover, it was the first case it had seen of an Authorised Push Payment (APP) fraud in the Islands "*where the bank received a change of payment details.*" Whilst it recognises that, at around that time, the "*UK banking industry was working towards* [a new] *voluntary code of practice as it recognised it needed to change … no such industry activity was underway in Guernsey suggesting we were facing a very different level of challenge.*"

- It agrees "*that the GFSC will expect our Guernsey branch colleagues to be given training in fraud and cyber risks so that they can recognise fraud …when they are servicing our customers.*" However, having reviewed relevant training material, the bank said that "*this specific type of APP fraud was not a feature of* [it]." In noting that the Guernsey branch's training material was aligned with UK training, the bank does not consider it is reasonable to expect it to have been part of the training in Guernsey.

- The GFSC warning notices I highlighted in my Provisional Decision "*make reference to banks being the victim of email scams, not customers. Therefore we do not see the direct relevance of this point ….*"

- "*The actions of [the complainant] have faced very limited challenge from CIFO.*" She should have been "*more conscientious and alert in her dealings with [the investment services company].*" There was a warning in [the investments services company's] email footers that clients should not act on any messages containing new payment details they might receive, and [the investment services company] might have alerted [the complainant] to this risk in other documents or in face-to-face meetings. Furthermore, the "*tone and style of the email [the complainant] received from the fraudster was notably different to her previous interactions with [the investment adviser].*" The bank did not see this correspondence before the transfer was made, and the email address [the complainant] replied to was different from [the investments services company's] genuine email address. Furthermore, it took [the complainant] six days to realise that [the investment services company] had not received the money – despite the fraudsters' message saying that '[the investment services company]' would be in touch once it had been received. Had [the complainant] followed the payment up more swiftly, the delay in the bank contacting [Bank B] to try to retrieve the money would have been lessened.

- It does not accept payment instructions by email, so [the complainant's] initial message to the bank's [redacted for anonymisation purposes] at 10.49am on 18 September 2018 giving advance notice of [the complainant's] intention to make a payment was not a 'payment instruction'. [The complainant] then "*sent further correspondence to [redacted for anonymisation purposes] on 18 September at*

11.37am to advise the payment details had changed, this was just 48 minutes after [the complainant's] first email which would not arouse suspicion with the follow up email being received so soon after [the complainant's] first email. … When [the complainant] visited the branch to formally provide the bank with her payment instruction as we had requested her to do, [the complainant] met with another colleague, [redacted for anonymisation purposes]. [The colleague] was not aware of the email interactions noted above between [the complainant] and [the bank]. [The colleague] completed the payment with the beneficiary details provided to her by [the complainant] where no mention of the change of beneficiary account details was raised." Both individuals have now left the bank, and this – coupled with the time that has since elapsed – "*limits the challenge we can present in respect of what may or may not have been said in interactions between [the complainant] and the Bank.*"

- "*The actions of [the investment services company] … have faced no challenge by CIFO …*" In acknowledging that the complaint has been made against the bank "*CIFO does have remit over Investment Management Companies in the Channel Islands and it does not feel unreasonable that CIFO explore the root cause of this complaint which is [the investment services company] who share their account details with customers online and without appropriate encryption.*" Despite [the investment services company's] awareness of APP fraud at the time, by their actions they "*knowingly transfer this risk to organisations like Lloyds Bank who ultimately fulfil customer transfer requests ….*"
- The bank felt that I had wrongly assessed [the complainant's] complaint in direct alignment with UK regulation, with "*this UK interpretation then being applied directly to a bank account held in Guernsey*." [The complainant's] account is in Guernsey, so the complaint should be assessed "*in relation to the different systems, controls, and regulatory framework within Guernsey*."

- Overall, my Provisional Decision was "*incorrect and unreasonable …* [and] *… should CIFO determine this complaint … in favour of [the complainant], this sets an unrealistic and unreasonable expectation on Lloyds Bank International in respect of the ongoing provision of payment services that we can provide customers, whilst not exposing the Bank to this significant imbalanced risk.*"

Findings

I have considered (and, where I had previously received it, re-considered) all the available evidence and arguments in order to decide what is fair and reasonable in the individual circumstances of this complaint.

I make a couple of introductory points. Firstly, [the investment services company] is indeed a financial services provider in the Channel Islands so it therefore comes within our scope. But whilst [the complainant] has complained to us about Lloyds she has not

complained about [the investment services company]. This means I cannot look into their actions when considering this complaint about Lloyds. I will nevertheless return to the broader point about the involvement of other parties in the overall matter towards the end of this Final Decision.

My second point is more fundamental to CIFO's approach to considering and determining complaints. Under the laws which give us our powers (for this case, the applicable law is the Financial Services Ombudsman (Bailiwick of Guernsey) Law 2014) we are required to reach our decisions having regard to – but not being bound by – any relevant law, regulation, codes of practice, and good industry practice. In addition, and overarching this, we are required to come to our decisions on the basis of what we consider to be fair and reasonable in the individual circumstances of each complaint we consider. That 'fair and reasonable' remit means it is appropriate for us to consider the applicable wider overall position, and to take account of whatever we consider to be relevant in order to reach what we assess to be a fair and reasonable outcome in the specific case – taking into account the perspectives of both parties to the complaint.

I make this point because, first of all, the bank has suggested that – in my Provisional Decision – I wrongly assessed [the complainant's] complaint in direct alignment with UK regulation, rather than against the background of [the complainant's] account being in Guernsey. I infer from what the bank has said that, in coming to my provisional conclusions on this Guernsey transaction, it considers I was wrong to have had regard to – for example – UK regulation and relevant developments in the UK relating to APP fraud.

However, I do not accept that – firstly as a matter of general principle for the reason I have just set out, and secondly because (even though the bank in the Channel Islands is a separate legal entity from the bank in the UK) its branch in Guernsey offers its customers a set of products and services which are largely similar to those which a UK customer might receive from an equivalent-sized branch office in the UK. Moreover, the bank has explained – for example – that its Guernsey training is aligned with the UK. So, overall, and unless there is (for example) an express regulation to the contrary, I consider it reasonable that a Guernsey customer should expect to receive the same broad level of service – and, where relevant, protection– from the bank's Guernsey branch as a UK customer would receive from an equivalent-sized branch in the UK when receiving a similar service.

In any event, it's also clear from our discussions with the GFSC – both in the past and more recently – that for a financial services provider such as Lloyds Banking Group which has a large UK presence, the regulator expects a bank in Guernsey to operate to at least the same levels and standards as its UK counterpart offices. Indeed, it would seem counter-intuitive to suggest otherwise, because that would imply an acceptance that a Guernsey customer might – in comparison – receive an inferior service. I cannot see

how it would be fair or reasonable to say that that could generally be right. Moreover, banks in the Islands are not insulated from what is happening in the UK, especially where there are clear parallels. Indeed, there is precedent which shows that they have followed and adopted the UK approach on issues which are broadly similar and which affect a number of their customers – for example, the assessment of Payment Protection Insurance complaints.

However, by way of my Provisional Decision I did not *directly* apply UK regulation to the circumstances of [the complainant's] case. Whilst it is of course true that – as a matter of first principle – a bank is expected to process payments in accordance with its customers' instructions, in my earlier assessment my starting point was the regulatory environment in Guernsey – which includes, where relevant, the expectation I have just outlined – and where the GFSC's Principles of Conduct of Finance Business require a bank, amongst other things, to "*act with due skill, care and diligence towards its customers*". In addition, section 7 of the GFSC's Code of Practice for Banks requires them to have risk management procedures in place – for their own benefit and, where applicable and by extension for their customers, to "*counter external fraud and other financial crime.*" This is further supported by Regulation 6C(b) of The Banking Supervision (Bailiwick of Guernsey) Regulations 2010 which says that a bank must undertake its business "*in such a manner as to ensure that permanent compliance and risk management functions are conducted in the Bailiwick to assess the risks and legal compliance of all business conducted from or within the Bailiwick.*"

I acknowledged in my Provisional Decision that the circumstances surrounding the warnings the GFSC had issued, dating back to 2013 and later repeated, about the potential use of compromised email accounts to commit fraud differed from the specific fraud in this complaint. I noted that these warnings might, at least in part, have been why Lloyds would not accept [the complainant's] payment instruction by email. But my primary point here was a broader one; because Lloyds, at the time of this transaction, did not accept email instructions from its customers it is clear that the bank was alert to such risks. So I consider Lloyds should have been similarly alert to the general risk to customers in relying on details contained in any email ostensibly received from a third party to make a payment – even leaving aside whether there had been an 11th hour change in the payment details. In my view this conclusion stands based on the information Lloyds in Guernsey has provided to me about its approach on the Island at the time, even without reference to what was happening in the UK.

But, in any event, I don't believe it's right to say that email intercept frauds were little known by late 2018, whether or not involving an 11th hour change in the payment details. For example, in August 2018 the UK Financial Ombudsman Service published its *Ombudsman News* edition 145 which focused on a range of complaints about fraud. It included an interview with an independent fraud investigator who said that high value APP frauds fall into three main categories, which included: "*Expected payment fraud,*

where the victim is expecting to make a high value payment for goods or services but inadvertently makes the payment to an account controlled by a fraudster, typically in response to an invoice or payment request attached to an email. I believe that this is the most common type of APP fraud and cases that I have seen include a property transaction (£144k), investments (£105k) and paying a genuine builder for work done (£44k)" (my underlining).

In other words, frauds of this specific nature had been known about in the UK for some time by 2018. So I am a little surprised by what the bank has said about its training material not covering it, both in the UK and, by extension, in the Islands. And focusing back on the Guernsey environment,it seems to me that this omission risks being incompatible with the bank's regulatory obligations to act with due skill, care and diligence, to counter external fraud and other financial crime, and to assess and manage risk effectively.

I note what the bank says about the work that was done in the UK following the Payment Services Regulator's policy statement in February 2018 and the introduction in May 2019 of the 'Contingent Reimbursement Model' (CRM) code for the victims of APP fraud. Lloyds Banking Group in the UK is a party to that code. But in acknowledging that the code does not formally extend to the Islands I believe it's nevertheless difficult to see how there might have been a materially 'different level of challenge' in Guernsey in and around 2018 such that it would be fair to disregard the provenance and intent of that code for customer payments made by banks in Guernsey.

Moreover, the UK CRM code was not the first step that had been taken in the UK to help tackle fraud and to protect banks' customers from financial harm. Whilst parts of the CRM code have undoubtedly strengthened that earlier protection, other parts of it have largely built on – or replicated to some extent – existing and well-established commitments and standards of good industry practice, as well as some UK legal and regulatory requirements. For example, the CRM code requires banks to detect, prevent and respond to APP scams. This is an expectation that had already been created in slightly different forms by other pre-CRM code voluntary arrangements such as the UK Banking Protocol and the British Standards Institute's October 2017 'Protecting Customers from Financial harm as a result of fraud or financial abuse – Code of Practice', as well as through anti-money laundering requirements and other legal considerations.

So, even before the CRM code was introduced I consider that Lloyds Banking Group will have known that banks in the UK had, for some time, been under largely similar regulatory obligations to banks in Guernsey – in particular, to have systems and procedures in place to counter external fraud and to seek to prevent both themselves and their customers from being victims of financial crime. This includes being sufficiently aware of the indicators of fraud and bringing them to the attention of

customers before they make high-value and/or unusual payments.

I make one final comment on this overall 'awareness' point relating to what the bank has said about the warnings [the investment services company] included in its email footers about clients not acting on messages containing new payment details. I will return to the question of whether [the complainant] should have identified and reacted to these warnings later in this Final Decision, but my point for now is that it's clear that – apparently unlike the bank – [the investment services company] evidently *was* aware of email intercept fraud, its risks, and wastaking steps to warn its clients about it in 2018.

With all of the above in mind I now turn to the specifics of the complaint.As I have already set out, I do so on the basis of what I consider to be fair and reasonable in its individual circumstances – and having regard to, in particular, the regulatory environment in Guernsey at the time.

Firstly, my understanding is that there is no dispute that [the complainant] remains out-of-pocket to the extent of the money Lloyds was unable to recover from [Bank B] in the UK, despite its swift action once alerted to the fraud.

Lloyds has explained that [the complainant] initially emailed the bank in the morning of 18 September 2018 to say she wanted to make her payment. Less than an hour later she emailed the same member of staff with revised payment details. The bank has said that because the second message came so soon after the first it would not have aroused suspicion. But I take a different view, firstly because I'm not persuaded that – of itself – this time gap between messages is particularly relevant but secondly, and arguably more importantly, because the revised payment details were provided so soon before the payment was to be made. Although I accept that the bank did not at that stage see the fraudsters' email – to which the new payment details were attached, and which the bank did receive – fraudulent revised payment details are rarely received well in advance. Instead, and to maximise their chances of success, fraudsters often send them at the '11th hour' – shortly before the payment is to be made in order to limit the possibility of detailed further enquiry.

But, as I have already noted, even if there hadn't been this 11th hour change in payment details I consider that – bearing in mind Lloyds' own stance on receiving such instructions by email and the broader consequent known risks inherent in relying on the details they contain – the bank should have identified the position and recommended to [the complainant] that she check with [the investment services company] before the transfer was made, to be sure that the beneficiary bank details she was about to use were correct. In fact, Lloyds had two opportunities to do this, both on 18 September and on 19 September.

Bringing this all together, therefore, and having regard to all that I have so far set out, I find – in summary – that:

- Lloyds was under a regulatory obligation in Guernsey to act with due skill, care and diligence, to counter external fraud and other financial crime, and to assess and manage risk effectively.

- The bank, as part of Lloyds Banking Group, will have had access to – and,as a result, the opportunity to have had a clear understanding of – broader and ongoing developments in relation to APP fraud.

- This particular type of APP fraud was known about by the financial services industry, not just in the UK but also in the Islands, at the material time.

- Lloyds in Guernsey was aware of the possibility that email accounts can be compromised – and, by extension, the risks of making payments just on the basis of an email instruction.

So, by not taking what I consider to have been appropriate and reasonable steps to counter the risk of financial crime in this case I find that Lloyds acted wrongly – and that, as a result, it deprived [the complainant] of the opportunity to take action to prevent the loss she has so far experienced.

There is, however, a further significant point I need to address before I come to my final conclusions. In its response to my Provisional Decision Lloyds said that "*the actions of [the complainant] have faced very limited challenge from CIFO*" and that she should have been "*more conscientious and alert in her dealings with [the investment services company.*" As I understand it, there are four main issues which concern the bank:

- the tone and style of the fraudsters' email in comparison with earlier emails [the complainant] had received from [the investment adviser];

- that she replied to the fraudsters' message on a different email address from [the investment adviser's] genuine email address;

- [The complainant] should have read and acted upon the warnings contained within [the investment services company] email footers (about clients not acting on any messages containing new payment details they might receive); and

- it took [the complainant] six days to realise the money had gone missing.

I said in my Provisional Decision that I understood Lloyds' point about the tone/style/grammar of the fraudsters' email which accompanied the new payment details, adding that I had explored this with [the complainant]. To be clear, I continue to see why – on looking back at the correspondence – it might have been possible for [the complainant] to have identified that something could have been amiss.

But I also believe we need to consider the position in context and as it was at the time because, in preparing to make her investment, [the complainant] received the fraudsters' email – ostensibly from [the investment services company] – which was just one of a broader exchange of messages. Also, the attached payment instruction was in the same format as the earlier one – with the same email address for queries. So, whilst I accept the point that the covering message differed a little from [the investment adviser's] own style, I do not consider – albeit after very careful consideration, and on balance – that there was enough in what [the complainant] received from the fraudsters for me to conclude that she was negligent in not questioning things at that stage. This includes the return email address, *[redacted for anonymisation purposes]*, which I accept differed slightly from *[redacted for anonymisation purposes]*. But again it was not, on the face of it, materially different – a technique intentionally adopted by fraudsters to try to limit the chance of the recipient noticing any change. Closer scrutiny has since identified the two differences, but I do not consider it appropriate to say that – in replying 'in the moment' to the message [the complainant] received by just clicking 'reply' – [the complainant] ought fairly be held accountable for not having noticed the substitution at the time.

Lloyds is right to say that there was a warning in the footer of the emails [the complainant] received from [the investment services company] about not acting on messages containing new payment details. I do therefore understand why the bank has raised the point. I have questioned [the complainant] about this, and I have also looked carefully at how the relevant information was presented.

At the time, [the investment services company's] email footer was lengthy – six paragraphs, with the relevant warning being in the last of those paragraphs. All the information was printed in a much smaller font than the remainder of the email – beginning with a fairly 'usual' paragraph about the confidentiality of the message. The four subsequent paragraphs were what might be described as standard/corporate information, so it's necessary to read right to the end of the footer to identify the warning paragraph. Furthermore, in light of what preceded it I consider it pertinent to note that the warning paragraph was not presented any more prominently than the earlier paragraphs – which, as I say, were much more 'standard' paragraphs and which, in my view, most people are relatively unlikely to read in detail. As I say, I do very much take the bank's point about this, but I can also see and understand what [the complainant] says about not having noticed the relevant warning. So, after very careful consideration and particularly in light of what I have set out about the way the warning featured in the overall footer, I have come to the

conclusion that it would not be fair or reasonable to say that [the complainant] should be held accountable for not having noticed the relevant section of the email footer at the time.

Lloyds has also asked whether [the complainant] was given the same warning by other means. But the bank has not provided anything to indicate she did –for example, whether [the investment services company] included the warning in client meetings or other documentation – and [the complainant] says she wasn't told about it in another way. I am, in the circumstances, content to accept what [the complainant] says.

Finally, Lloyds raises the question of delay in 'raising the alarm'. This, of course, goes to the question of whether the bank might otherwise have been able to recover a larger amount of the money from [Bank B] – rather than whether the transfer should have been made at all using the fraudulent payment details. The six days encompassed a weekend, so the effective period was four business days. As part of the email exchange with the fraudsters [the complainant] had confirmed to '[the investment services company]' that the payment had been sent, so – in these specific circumstances – even though the fraudsters' message had said that '[the investment services company]' would be in touch once the money had been received I do not see that this time period should necessarily have led [the complainant] to have followed the payment up much more quickly, if at all, than she did. Whilst banks are familiar with the timeframes for different types of transfers – some of which are made the same day, but others take several days – customers are often less so.

Bringing these four points together, therefore, in order to consider the bank's contention that [the complainant] acted with contributory negligence in respect of one or more of them, for the reasons I have explained I find I am unable to conclude that [the complainant] did. Were there opportunities for [the complainant] to have identified the potential of fraud; yes, there were. But, in these specific circumstances, should her not having done so offset the bank's failure, as the professional financial services provider, to have done so? In my view, no it doesn't. Had the specific circumstances been different I might have come to a different view on this – although, as I have already indicated, it's relevant to bear in mind that effective fraudsters are adept at taking careful steps to try to make sure that the customer does not notice that emails have been intercepted and that material details have been substituted.

I make one final observation. Lloyds has said that, by my upholding this complaint, it will "*set an unrealistic and unreasonable expectation on Lloyds Bank International in respect of the ongoing provision of payment services that we can provide customers, whilst not exposing the Bank to this significant imbalanced risk.*" However, I find it difficult to agree with this. Whilst it is not for CIFO to tell a financial services provider how to run its business, banks in the UK have – for some time now, and as I have set out above – been required to comply with relevant UK regulation and codes ofpractice

in order to seek to prevent fraud and to protect their customers. So a reasonable approach might be for Lloyds to consider adopting the procedures and processes which branches of UK banks are continually developing and implementing in order to comply with that regulation –and, in particular, the principles of the CRM code.

So, for the reasons I have explained, I propose to uphold this complaint. However, before I set out how it should be settled there are two further points I need to repeat from my earlier Provisional Decision.

The first is that the maximum amount I can formally award a complainant in any individual case is £150,000. [the complainant] is currently out-of-pocket by more than that. Whilst I can recommend that a bank pays any excess, it is up to Lloyds alone to decide if it will pay any recommended amount; I cannot require it to do so.

My second point is that it is for Lloyds to consider if it wishes to approach any of the other involved parties ([the complainant] apart, of course) to seek to share overall liability. That said, if the bank were to do so it must not delay settlement with [the complainant]. In other words, if [the complainant] accepts this Final Decision the bank must settle her claim directly and without delay – and then separately consider if it wishes to make a claim against any other involved party.

Final Decision

For the reasons I have explained, my Final Decision is that I uphold thiscomplaint.

In settlement of it, Lloyds Bank Corporate Markets plc, trading as LloydsBank International (Guernsey branch) should pay [the complainant] the sum of £150,000. I further recommend that Lloyds Bank Corporate Markets plc, trading as Lloyds Bank International (Guernsey branch) should:

1 – pay to [the complainant] the sum of £14,113.86; and

2 – pay interest to [the complainant], at an annual rate of 8% simple, on the total sum of £164,113.86 from 19 September 2018 to the date of settlement.
This rate of interest is in line with CIFO's usual approach in circumstances such as these.

Next steps for [the complainant]

[The complainant] must confirm whether she accepts this Decision either by email to ombudsman@ci-fo.org or by letter to the Channel Islands Financial Ombudsman, PO Box 114, Jersey, Channel Islands, JE4 9QG, **within 30 daysof the date of this Decision** – that is, by 11 November 2020. The Decision will become binding on [the complainant] and Lloyds if it is accepted by this date.

However, if there are any particular – and exceptional – circumstances which prevent [the complainant] from confirming her acceptance before the deadline, [the complainant] should contact me with details. I may be able to take these into account, after inviting views from Lloyds, and in these circumstances the Decision may become binding after the deadline. I will advise both parties of the status of the Decision once the deadline has passed.

Please note there is no appeal against a binding Decision, and neither party may begin or continue legal proceedings in respect of the subject matter of a binding Decision.

If we do not receive an email or letter by the deadline, the Decision is not binding. At this point [the complainant] would be free to pursue her legal rights through other means.

David Millington
Ombudsman
Date: 12 October 2020

COPY Ombudsman Provisional Decision
CIFO Reference Number: 18-000424
Complainant: [the complainant]
Respondent: Lloyds Bank (International Services) Limited

It is the policy of the Channel Islands Financial Ombudsman (CIFO) not to name or identify complainants in any published documents. Any copy of this decision made available in any way to any person other than the complainant or the respondent must not include the identity of the complainant or any information that might reveal their identity.[1]

A decision shall constitute an Ombudsman Determination under our law.

Complaint

[The complainant] complains, in summary, that Lloyds Bank (International Services) Limited failed to make adequate checks to ensure that a payment she had asked it to make was transferred to the correct beneficiary.

Background

Following her divorce some years ago, [the complainant] received an income from her father's trust to help support herself and her children. She explains that the trust was dissolved in May 2018, leading to her receiving a lump sum – part of which was to support day-to-day living, and part was to be invested to provide financial security for the future.

[The complainant] approached an investment services company, [redacted for anonymisation purposes], for advice. Their investment adviser, [redacted for anonymisation purposes], recommended she invest in [the fund]. As a result, on 18 September 2018 [the complainant] asked Lloyds to pay £434,000 from her accountto '[redacted for anonymisation purposes]'. [The complainant] initially did so by email, to which she attached the information she'd received from [the investment services company] about [the fund's] bank account at [Bank A]. But a little over an hour later, [the complainant] sent a further email to the bank – in which she said the 'transfer details' had changed. [The complainant] attached an updated note she had (apparently) received from [the investment adviser] at [the investment services company], which said the payment should be made to [the fund's] account with [Bank B].
Lloyds required [the complainant] to sign an authority to make the payment, and she visited its Smith Street, Guernsey branch on 19 September 2018 to do so. The authority was completed using the updated account details for [the fund], and the bank made the payment from [the complainant's] account.

Six days later, on the morning of 25 September 2018, the bank received an email from [the complainant] saying the money had not arrived. Later that morning, [the

investment services company's] Money Laundering Reporting Officer visited the bank and said they believed [the complainant's] email account had been 'hacked'. [The investment services company] had *not* provided her with updated bank details for the transfer. Lloyds subsequently completed an 'Authorised Push Payment Scam Notification Form', which it sent to [Bank B], and it asked for the money to be returned. However, [Bank B] was not able to recover the full £434,000. Between November 2018 and February 2019 [Bank B] returned a total of £269,886.14 to Lloyds, leaving £164,113.86 outstanding.

[The complainant] complained to Lloyds, saying – amongst other things – that she "*would expect Lloyds to have the expertise to note suspicious behaviour. It is not an excuse to state that you simply do what the customer requests with the bank details they give to you. The customer places his or her trust in you to look after his or her funds to the best of your ability and with significantly more awareness of possible risk and fraudulent behaviour than the customer himself or herself.*"

By way of its letter to [the complainant] dated 8 January 2019 Lloyds said – amongst other things – that "*the onus is on a customer to validate the bank account details of the beneficiary. In making this payment, we acted on the instructions provided by you during your visit to our St Peter Port branch, which were accompanied by your signed authority to debit your Island Premier Savings account. Accordingly, we would not be liable for any amount you have paid to this recipient should you be unable to recover further money from the recipient bank.*" The bank has continued to maintain that position.

Findings

I have considered all the available evidence and arguments to decide what is, in my opinion, fair and reasonable in the individual circumstances of this complaint. Where appropriate, I reach my conclusions on the balance of probabilities – in other words, what I consider is most likely to have happened, in light of the available evidence and the wider surrounding circumstances.

The potential loss of over £160,000 – whatever the circumstances – is likely to be a severely distressing, and potentially life-changing, event for most people. It's clear that Lloyds acknowledges the distress caused to [the complainant] as a result of the money having been sent to what we now know was a fraudulently-opened account in the UK, rather than [the fund's] own account in Jersey. It's also clear that Lloyds acted swiftly once the issue came to light; within a matter of a few hours from first being notified of a potentialproblem Lloyds had liaised with [Bank B] and had received confirmation that the beneficiary's account had been 'secured' – leading, over the succeeding few months (and through a considerable amount of further liaison between Lloyds and [Bank B]) to the return of almost £270,000.

The question I need to address, however, is this: in making the payment was it right for

Lloyds simply to have relied on the information [the complainant] had provided, or should it – in these specific circumstances – have taken some other action which, had it done so, might have prevented the fraud and the resultant loss which [the complainant] has so far experienced?

The starting position is that a bank is expected to act in accordance with its customers' instructions, and to make the payments it's asked to make. This is, in essence, what the bank is saying – and, by extension, that it is for the customer alone to be sure that the details he or she provides are correct. Lloyds has in fact gone a little further than that here, because it has also said the fraud was facilitated by a combination of other things outside its control – including (but possibly not limited to): [Bank B] in the UK opening a fraudulent account; [the investment services company's] and/or [the complainant's] email accounts being hacked; and the 'warning signs' (style/tone/grammar) in the email she ostensibly received from [the investment adviser] at [the investment services company] – which incorporated the new payment instructions, and which the bank suggests should have put [the complainant] on notice that the message may not have been genuine.

On the other hand, I believe [the complainant] is right to identify that banks might reasonably be expected to be aware – arguably more so than their customers – of potentially- fraudulent behaviour, and to take appropriate action to help prevent fraud from taking place. Banks are, of course, also subject to regulation and the expectations of their regulator; in this case, the Guernsey Financial Services Commission (GFSC).

Over the past few years, instances of this type of 'email intercept' fraud have been on the increase, and they have been widely reported in the media. Their typical pattern is what happened here; an 'eleventh hour' change to the payment details. Lloyds accepts that it knew the payment details had changed (because [the complainant] forwarded to the bank both sets of information), although it did not see the email which accompanied the second set until some time later. But the bank has also told me this was the first instance of its type it had experienced in Guernsey – so it would not have expected its staff to have suspected that anything might have been amiss from the 'eleventh hour' change, and neither would it have been put on alert by the beneficiary's bank account changing from Jersey to the UK.

If these circumstances had arisen at a branch of Lloyds in the UK, both the law and relevant regulation set out by the UK financial services regulator (the Financial Conduct Authority) would have broadly supported [the complainant's] view about what the bank might reasonably have been expected to be aware of. By late 2018, this type of fraud was well-known in the UK. So, the question therefore becomes: to what extent, if at all, should a bank in Guernsey have been under similar regulatory (if not legal) expectations at that time – in particular, bearing in mind that Guernsey banks are regulated by the GFSC, not the UK Financial Conduct Authority?

The Guernsey financial services regulatory environment is made up of specific regulation issued by the GFSC (which includes, for example, warning notices to financial services providers) and, importantly, a general expectation that – where appropriate, and in the absence of anything specific or to the contrary – a financial services provider will act to at least any equivalent UK regulatory standards. This principle particularly applies to an Island branch of a UK clearing bank – where, for example, the GFSC also expects Guernsey branch staff to receive the same level of training as UK branches. What this means therefore, is that – in order to reach a fair overall outcome in this complaint – it is appropriate for me to consider relevant UK regulation alongside any direct regulation from the GFSC.

UK regulation relevant to the circumstances of this case has developed over several years. It includes the longstanding duty to counter the risk that banks may be used to further financial crime, which has been supplemented by periodic papers setting out examples of good and poor practice found when reviewing measures taken to counter financial crime. Underpinning all of this are the overarching principles that banks are required to conduct their "*business with due skill, care and diligence*" and to "*pay due regard to the interests of* [their] *customers.*" This includes being on the 'look out' for transactions which, as well as being unusual for any individual customer, contain one or more 'hallmarks' of a potential fraud.

The Financial Conduct Authority (and the UK Financial Ombudsman Service) also expects banks to act in accordance with good industry practice – much like CIFO does. That includes identifying and assisting customers who might be vulnerable to fraud – and, arguably more relevantly here, identifying and helping to prevent transactions which could involve fraud or be the result of a 'scam'.

In addition, over the years the GFSC has itself issued warnings to Guernsey financial services providers about the potential use of compromised email accounts to commit fraud. For example, as far back as September 2013 the GFSC issued a warning about fraudsters intercepting customers' email accounts – about messages which appeared to come from the customer but where, in fact, the email account was being controlled by a fraudster. That warning was repeated in March 2015. I recognise that the precise circumstances outlined by these specific warnings differ a little from the particular fraud in this case (and may well have been part of the reason why Lloyds wanted to see [the complainant] in person rather than just accept email instructions to make the payment). But notwithstanding that, and in light of the broader overall circumstances, on balance I find that – by September 2018 – the bank should reasonably have been aware of the underlying risk to [the complainant] in relying on an email ostensibly from [the investment services company] providing very recently-revised payment details for such a high-value transaction.

Putting this another way, what I consider all of this means is that – at the time of this

payment – Lloyds was under a regulatory obligation to have ensured that its staff in Guernsey both understood the potential risks of email instructions/intercepts, and that they were no less aware of potential frauds than their colleagues in the UK. Indeed, I consider it arguable that – given the nature of the financial services environment on the Island – the bank's Guernsey branch might have been expected to have been *more* aware of the risks of fraud, especially for high-value payments such as this, than a branch of the bank in an equivalent-size town in the UK. And because the GFSC will have expected the bank to have provided [the complainant] with no less a service than from any branch in the UK, taking account of all relevant regulatory guidance and obligations – both issued by the GFSC and originally emanating from the UK – that means recognising this type of 'email intercept' fraud and raising it with the customer before the payment was made.

If Lloyds had done so, and if it had asked [the complainant] to check the second set of payment instructions with [the investment services company], I consider this fraud would have quickly come to light and the payment would not have been made to the fraudsters' account. It follows directly from this that, but for Lloyds not questioning the 'eleventh hour' change in the payment details, I find that [the complainant] would not be out-of-pocket in the way she is today.

In saying this I do recognise that there are other parties to this complaint, including [the investment services company] – where Lloyds has questioned why [the complainant] has not complained about them (on the basis that it may have been their email account, rather than [the complainant], which was 'hacked'). But it is not for me to tell complainants who they should complain about; rather, it is for me to consider the complaint that is made to CIFO. I can additionally see that [Bank B] in the UK had a part to play in facilitating the transaction, but I cannot consider a complaint about a UK branch of a bank.

I also acknowledge – and understand – Lloyds' point about the tone/style/grammar of the email [the complainant] received from the fraudsters when they gave her the new payment details, such that that might reasonably have put her on notice that it might not have been genuine. I have explored this point directly with [the complainant], as a result of which I am – on balance – satisfied that, whilst she might have identified that something was amiss I can equally appreciate why she did not do so. So, after very careful consideration, I do not accept that – by not having questioned things at that stage – she should be required to accept liability herself for the payment being made as it was.

I should also add, for the sake of completeness, that whilst I can see it's possible (albeit maybe slightly unusual) for a Channel Islands-based investment company to have an account in the UK, of itself – and on balance – I don't consider that that would, in this case, necessarily have been enough to have alerted Lloyds to the potential of fraud.

I say this notwithstanding the evidence I have received from [the complainant] suggesting that Lloyds was familiar with making payments to [the fund] and was likely to have known they banked at [Bank A]. In my view, the much more compelling point in this case is the bank not having identified the possibility of an 'email intercept' fraud, and not taking appropriate action to question/seek to prevent that.

So, for the reasons I have explained, I am minded to uphold this complaint.

However, before I set out how I consider the complaint should fairly be settled there are two further points I need to address.

The first is that the maximum amount I can formally award a complainant in any individual case is £150,000. [The complainant] is currently out-of-pocket by more than that. Whilst I can recommend that a bank pays any excess, were I to make a formal determination of this case it would be up to Lloyds alone to decide if it would pay any recommended amount. I could not require it to do so, although I would naturally hope it would.

My second point is that, on the assumption that the matter can be settled between Lloyds and [the complainant] in the way I set out below, it would be for Lloyds to consider whether it wished to approach any of the other involved parties ([the complainant] apart, of course) to seek to share overall liability. That said, if the bank were to do so it must not delay any settlement with [the complainant]. In other words, the bank should settle [the complainant's] claim directly – and then separately, and subsequently, consider approaching any of the otherinvolved parties.

Provisional Decision

For the reasons I have explained, my Provisional Decision is that I am minded to uphold this complaint. To settle it, I consider that Lloyds Bank (International Services) Limited should pay to [the complainant] the sum of £150,000. I further recommend that Lloyds Bank (International Services) Limited should:

1 – pay to [the complainant] the sum of £14,113.86; and

2 – pay interest to [the complainant], at an annual rate of 8% simple, on the total sum of £164,113.86 from 19 September 2018 to the date of settlement.

This rate of interest is in line with CIFO's usual approach in circumstances such as these.

However, if either party disagrees with my Provisional Decision the matter may be reviewed again, after which I will complete a formal determination.

If either party wishes me to undertake a further review and complete a formal determination, and considers they have additional evidence or observations which they have not already provided which might inform that further review, these should be sent

to me at ombudsman@ci-fo.org to reach me within 30 days of the date of this Provisional Decision – that is, by 12 June 2020 at the latest.

David Millington
Ombudsman

Date: 13 May 2020