

EMPLOYMENT TRIBUNALS

Claimant: Mrs C Sharpe

Respondent: Directa (UK) Ltd

Heard at: East London Hearing Centre

On: 7 March 2019

Before: Employment Judge Ferguson

Representation

- Claimant: Ms G Cullen (Counsel)
- Respondent: Mr M Stephens (Counsel)

RESERVED JUDGMENT

It is the judgment of the Tribunal that the Claimant's complaint of unfair dismissal fails and is dismissed.

REASONS

INTRODUCTION

1. By a claim form presented on 30 October 2018 the Claimant brought a complaint of unfair dismissal. The Respondent defended the claim. The issues to be determined are:

- 1.1 What was the reason for the Claimant's dismissal and was it a fair reason under section 98(1)-(2) of the Employment Rights Act 1996?
- 1.2 If the reason for dismissal was Some Other Substantial Reason:
 - (a) Was the decision to dismiss within the range of reasonable responses?
 - (b) Did the Respondent follow a fair procedure in all the circumstances?

- 1.3 If the reason for dismissal was conduct:
 - (a) Did the Respondent believe that the Claimant committed the misconduct in question?
 - (b) Were there reasonable grounds for that belief?
 - (c) Did the Respondent carry out as much investigation as was reasonable in all the circumstances of the case?
 - (d) Did the Respondent follow a fair procedure in all the circumstances?
 - (e) Was the decision to dismiss within a range of reasonable responses?
- 1.4 If the dismissal is found to be unfair, would it be just and equitable to reduce any award of compensation having regard to the principle in *Devis v Atkins*?
- 1.5 If the dismissal is found to be unfair, should there be a reduction under section 122(2) and/or section 123(6) of the Employment Rights Act 1996?

2. On behalf of the Respondent I heard evidence from Steven Smith, Martin Storey and Leslie Dennison. I also heard evidence from the Claimant.

FACTS

3. The Respondent company supplies industrial consumables to businesses across the UK and internationally. It employs approximately 60 people. The Claimant commenced employment with the Respondent as a Management Accountant on 5 November 2012. The Respondent banks with NatWest and the Claimant was responsible for managing the relationship with NatWest as well as the company's online banking via a service called Bankline. The Claimant had primary responsibility for Bankline and logged into the service every day. Her line manager, Cheryl Thompson, also had access to Bankline.

4. On 22 May 2018 the Respondent was the victim of a fraud which involved two different people telephoning the Respondent pretending to be from NatWest and gaining access to the Respondent's bank account via Bankline.

5. In the morning Ms Thompson received a call from a woman who said she was Amira from NatWest. "Amira" said that Ms Thompson's bank account access had been frozen due to a customer requesting a refund of £1,307.14. Both Ms Thompson and the Claimant knew that this exact sum was due from a customer and they had been chasing the payment from some time. The Claimant's evidence to the Tribunal was that they both considered this was information that only NatWest could know. Ms Thompson told "Amira" that the refund should not be processed.

6. At 1.24pm the Claimant sent an email to the Respondent's bank manager, Darren Clark, copied to two others at NatWest, entitled "Recalled deposit and locked account". She said they had received a call from "Amanda Khan" regarding a recalled deposit of £1,307.14. She said they disputed the reason for the recall and attached an invoice to

prove that the amount was due. She asked him to arrange "the release of the account" immediately and to cancel the recall.

7. At around 1.30pm the Claimant received a called from "Andrew", who said he was from NatWest. He had wanted to speak to Ms Thompson but she was on her lunch break so the Claimant took the call. Andrew knew both the Claimant's and Ms Thompson's names and referred to the refund of £1,307.14. He said he was following up on the call from Amira. He said he would arrange to release the account and reject the refund. During a lengthy call, which according to the Claimant included discussion of the weather, "Andrew" asked the Claimant to confirm her ID for Bankline, which she did. He then asked her for two digits from her password, which she also provided. Finally, he asked the Claimant to provide a "challenge number", i.e. the number produced when using her Bankline card and mobile card reader. The Claimant did so.

8. At 1.51pm Darren Clark replied to the Claimant's email asking her to call him. She replied at 1.52pm saying "Hi Darren, currently on call to Andrew who is arranging release of account and rejection of recall". Mr Clark responded at 1.58pm saying he was confused. The Claimant responded, "Hi, they rang me after I sent the email, on phone for $\frac{3}{4}$ hour."

9. At around 2pm the Claimant was still on the phone to Andrew when Ms Thompson received a genuine call from Mohammed at NatWest Bankline Security. He said that the Claimant's access to Bankline had been suspended. He said he had received a call from someone purporting to be the Claimant and he needed Ms Thompson to check if it really was the Claimant he had spoken to. According to a transcript of the call he said if "it turns out to be somebody – a fraudster and she turns out not to recognise my name at all, can you please call us back and let us know". He provided a number and Ms Thompson said she would check and let him know.

10. After this call Ms Thompson went to the Claimant's desk. The Claimant was still on the phone to "Andrew" but paused the call. Ms Thompson asked her if she had spoken to Mohammed, without explaining the content of the conversation with Mohammed. The Claimant said she had not spoken to him. The Claimant and Ms Thompson both noted that the number Andrew was calling from was the same number Mohammed had left to return his call.

11. It is a technique of fraudsters, known as "vishing", to clone a phone number so that a call appears to come from that number.

12. By this time Andrew had told the Claimant that her card had not worked in releasing the account. The Claimant told Andrew that Ms Thompson had returned to the office and asked if he still wanted to speak to her. He said he did. The Claimant handed the phone to Ms Thompson and explained that her card had not worked in releasing the account. Andrew asked Ms Thompson to provide the same details the Claimant had provided, i.e. two digits from her password and the "challenge number". Ms Thompson provided both. Andrew told Ms Thompson she should wait 20 minutes before checking Bankline again.

13. Ms Thompson did not return Mohammed's call.

14. After 20 minutes the Claimant checked her account access and noted that it was still frozen. She called the NatWest relationship team and was made aware of a transfer of

£49,850 out of the Respondent's account. Two future payments had also been set up. The Claimant called the fraud team and spoke to Mohammed. NatWest cancelled the future payments. The payment of £49,850 could not be stopped and has never been recovered.

15. It is not in dispute that a security warning is displayed every time a customer logs onto Bankline. It states:

"We will never ask for PINS, passwords or smartcard security codes over the telephone in any circumstances. If in doubt, call the Bankline Helpdesk".

16. It is also not in dispute that the Claimant engaged in a Bankline security review with Mr Clark in early April 2018. Following a telephone conversation with Mr Clark, the Claimant received an email from Ian Collier, Assistant Relationship Manager at NatWest, on 10 April 2018. This attached a security poster, which Mr Collier said could be shared amongst the Claimant's team who use Bankline. The email also attached a document entitled "Bankline Security Review", which made recommendations for improving the Respondent's online banking security, including introducing payment limits and restricting destination countries. The Claimant accepts that she did not open the poster or forward it to anyone else at the Respondent. She also accepts that she did not implement the recommendations in the review document. She could not explain why.

17. The security poster includes the following "tips to help keep your business safe when using Bankline":

"We will never ask for your full PIN & password online: only 3 random digits from each are needed to log in"

"We will never ask you for smartcard codes or any digits from your PIN & password over the telephone: beware of imposters"

"We will never ask for smartcard codes to log in: these codes are used to authorise payments"

18. Those three warnings were also set out at the foot of Mr Collier's email.

19. On 23 May 2018 a meeting took place to discuss the fraud of the previous day. This was attended by Leslie ("Dave") Dennison (the Respondent's Managing Director), Martin Storey (Senior Director), Ms Thompson and the Claimant. Subsequently Steve Smith, Sales Director, was appointed to conduct an investigation. He made enquiries with the bank and obtained statements from the Claimant and Ms Thompson. There was no real dispute about what had happened.

20. By letter dated 24 May 2018 Darren Clark of NatWest wrote to Mr Dennison denying any liability for any loss arising out of the fraudulent payment. The letter states:

"We believe the Company has been the subject of a 'vishing' attack. In this case you provided log in credentials and a challenge code(s) to a third party purporting to be from the Bank leading to the loss. This is a breach of the security terms of use of Bankline. Had the security messages issued via Bankline been heeded, and appropriate precautions taken as recommended by the Bank in various security advice notifications and communications, we are confident that the fraud would have been prevented.

We can confirm that the payment from your account was not processed as a result of any breach of the Bank's own IT systems. Bankline is customer administered system where its administrators can set their own limits and controls for users."

21. Mr Smith conducted an interview with the Claimant on 4 June 2018. He referred the Claimant to Clause 22 of the company handbook, which states:

"22. TELEPHONE, COMPUTER SECURITY, INTERNET AND E-MAIL ACCESS AND MISUSE

There are business and legal requirements for having a telephone, computer security and misuse policy. Each employee has a responsibility for the protection of Company information and must therefore make himself/herself familiar with the relevant requirements in respect of telephone, computer security and misuse. All employees must ensure passwords and security passes remain secure and private. Each employee is responsible for reporting any breach of telephone or computer security, no matter how trivial. The information held on computers must be correct so that it can be relied upon by the Company and its customers. Any release or use of information must be authorised by a Senior Manager or Director and must be with the agreement of the person responsible for the data."

22. The Claimant said she was familiar with it. She also said she was familiar with the Bankline tips for keeping businesses safe. When asked if she had anything further to add, the notes of the meeting record that she said:

"How did the initial information come to light, how did the fraudster know £1307.14 had been paid in the first place? . This was the main reason everything was so believable and started it all off.

Prided myself on being accurate and meticulous and I am gutted I got caught out.

• • •

4 people should take the blame for this Christine [herself] and Cheryl for being gullible and Mohammed and Darren Clarke

Disappointed that Darren Clarke hasn't been included in the bank investigation as he had the opportunity as well to freeze the account he is conspicuously absent from the report"

23. Mr Smith also interviewed Ms Thompson on the same day. She said that when she spoke to "Andrew" she thought she was unlocking the Claimant's account on Bankline "as asked by Christine". On 19 June 2018 Ms Thompson wrote a letter to Mr Dennison in which she said she would "deeply like to apologise". She said she felt she was "misguided and foolish to trust Christine and her ability to carry out a simple task well within her

competencies". She also said she felt "isolated and unsupported from the management team".

24. On 20 June 2018 NatWest wrote a further letter to Mr Dennison, apparently responding to a complaint about the level of service received from the bank. The letter refers to the warnings issued by the bank about calls asking for login details. It mentions the security review and the poster that had been sent to the Claimant prior to the fraud with advice about 'vishing'. The letter also refers to the fact that Mohammed's call was not returned and Bankline security details were provided to the fraudsters against the bank's advice. The letter advised that this was "a matter for you to take up within your business as you consider appropriate".

25. On 25 June Mr Smith wrote to the Claimant inviting her to a disciplinary hearing on 5 July, to be conducted by Martin Storey. The allegations were set out as follows:

"That on 22nd May 2018 you disclosed highly confidential information to unauthorised persons who were seeking to cause harm to the Company, specifically:

- a. The Company's Name on Bankline;
- b. Its User ID;
- c. Its User Code;
- d. Digits from your Password;
- e. Digits from your PIN number and
- f. Codes from the Card Reader.

That you failed to comply with the following provisions under paragraph 22 of the Company's Employee Handbook:

a. All employees must ensure passwords and security passes remain secure and private.

b. Each employee has a responsibility for the protection of Company information and must therefore make himself/herself familiar with the relevant requirements in respect of telephone, computer security and misuse.

That you failed to comply with the warning notice for BankLine 'keep your business safe';

That you failed to observe the warnings set out in NatWest's poster emailed to you on 20th April 2018;

That you failed to telephone Darren Clark of NatWest as requested by his email timed at 13.51 on 22nd May 2018;

That you subsequently requested your senior manager to assist you to unlock BankLine for the benefit of unauthoritsed persons who were seeking to harm the Company;

That at the time you did so you failed to explain to your senior manager:

- a. That you had previously disclosed the information set out at (a)-(f) above by telephone, and
- b. That you had received but not complied with a request to telephone Darren Clark at NatWest."

26. Ms Thompson was also invited to a disciplinary hearing on the same day, also to be conducted by Mr Storey. The allegations against her were:

"That on 22nd May 2018 you assisted a junior colleague to facilitate an unauthorised transaction to unauthorised persons who were seeking to cause harm to the Company.

That you did so without making sufficient enquiries to satisfy yourself that you were facilitating a genuine transaction."

27. The disciplinary hearings ultimately took place on 25 July 2018. During the Claimant's hearing, when asked about the warnings on the Bankline login page, she said it's "one of those things you don't see" because it comes up every day. When referred to clause 22 of the company handbook the Claimant said that she had read it only after Mr Smith showed it to her. The Claimant then said,

"I do not deny that I handed out information I shouldn't have done, I've always said that, never tried to hide it, never tried to explain it, well I have tried to explain it obviously..."

28. When asked about the email from Mr Collier at NatWest, which the Claimant pointed out was on 10 April, not 20 April, the Claimant accepted receiving it and said that she had not opened the attachments. She accepted that the bank would never ask for the "challenge codes" but said she truly believed it was the bank on the phone and in context "it seemed perfectly plausible". At the end of the hearing the Claimant said, "just give us a warning get it over and done with and let us get on with our jobs".

29. By letter dated 3 August 2018 Mr Storey informed the Claimant that her employment would be terminated on notice. She was paid in lieu of notice, so her dismissal took effect on 3 August. Mr Storey noted that the Claimant was employed in a senior role and that a high level of trust was placed in her. He believed "it should have been apparent to you at some point during a call of between 45 minutes to an hour that you were being asked to disclose information that you knew the Bank would not ask you to disclose." He also noted that the Claimant did not apologise and "sought to put the majority of the blame" on Ms Thompson. He considered that she failed to appreciate the seriousness of her actions. He said he took on board that she did not intend to harm the Company and did not act deliberately, but his view was that her failings were very serious.

30. Ms Thompson was given a written warning to remain on her file for 12 months. Mr Storey accepted that she was brought into a situation about which she had limited information, but said that she ought to have made enquiries to satisfy herself why she was being asked to unlock the Bankline account and by whom, and why the Claimant's profile had been locked.

31. On 7 August 2018 the Claimant telephoned the Respondent's office asking to speak to a colleague, Caroline, and giving the name "Angela", which she knew was the name of a customer. Once she had been put through she told Caroline who she was and asked if Ms Thompson was still working for the Respondent.

32. The Claimant appealed against her dismissal and the appeal was heard by Mr Dennison. Mr Dennison sent Ms Thompson a copy of the Claimant's appeal letter and asked her to comment on the assertions in it. The appeal hearing took place on 4 September 2018. By letter dated 11 September 2018 the appeal was dismissed. Mr Dennison said he supported the dismissal "because the Company's faith in your abilities to carry out a job function that requires a very high level of responsibility and trust was damaged beyond repair". He also referred to the Claimant's dishonest and underhand behaviour in lying about her identity to obtain information about Ms Thompson.

THE LAW

33. Pursuant to section 98 of the Employment Rights Act 1996 it is for the employer to show the reason for the dismissal and that it is one of a number of potentially fair reasons or "some other substantial reason". A reason relating to the conduct of an employee is a fair reason within section 98(2). According to section 98(4) the determination of the question whether the dismissal is fair or unfair "depends on whether in the circumstances (including the size and administrative resources of the employer's undertaking) the employer acted reasonably or unreasonably in treating it as a sufficient reason for dismissing the employee" and "shall be determined in accordance with equity and the substantial merits of the case."

34. In misconduct cases the Tribunal should apply a three-stage test, set out in *British Home Stores Ltd v Burchell* [1980] ICR 303, to the question of reasonableness. An employer will have acted reasonably in this context if:-

- 34.1 It had a genuine belief in the employee's guilt;
- 34.2 based on reasonable grounds
- 34.3 and following a reasonable investigation.

The Tribunal must then consider whether it was reasonable for the employer to treat the misconduct as a sufficient reason for dismissal. In respect of each aspect of the employer's conduct the Tribunal must not substitute its view for that of the employer but must instead ask itself whether the employer's actions fell within a range of reasonable responses (*Iceland Frozen Foods Ltd v Jones* [1982] IRLR 439).

CONCLUSIONS

35. Was the Claimant dismissed for a potentially fair reason? There is little between the parties on this issue. Claimant argues that her dismissal was for a reason related to her conduct, whereas the Respondent says it was either conduct or "some other substantial reason", namely the "terminal loss of trust in the Claimant". In my view they come to the same thing. The Claimant was dismissed primarily for disclosing online banking security details contrary to the bank's advice, causing significant loss to the Respondent. That is a reason that relates to her conduct and is therefore a potentially fair reason for dismissal. Conduct does not necessarily mean deliberate conduct and can encompass serious negligence.

36. The Claimant does not take any issue with the genuineness of the Respondent's belief or the grounds for that belief. That is unsurprising given that there was no significant dispute at the time of the Claimant's dismissal as to what had happened.

37. The Claimant does argue, however, that the investigation was insufficient. She says that the investigation should have included enquiries as to how the fraudsters had obtained information about a debt that was owing to the company. She also says that there should have been greater focus on the lack of training received by the Claimant. I do not find merit in either argument. The source of the fraudster's information was not relevant to the Claimant's culpability. It was never disputed that they had somehow managed to obtain correct information about a debt that was owed to the company. Mr Storey found, and indeed the Claimant accepted, that notwithstanding that context the security details should never have been disclosed. It was naïve of the Claimant to place so much significance at the time, and indeed that naïveté has persisted to the Tribunal hearing, on the fact that the fraudsters knew the precise amount owed by the customer. She believed this was information that only the bank could have known, but of course the customer also knew it and could have disclosed it to anyone, whether deliberately or inadvertently. The fraudsters successfully used this one piece of information to gain the Claimant's trust. Whatever the source of it, she should have been alert to the possibility that the callers were not genuine.

As to training, this is something of a red herring. The Claimant has never disputed 38. that she was aware of the bank's warnings not to disclose password or challenge code information over the telephone. Even if the security warnings displayed on the login page had lost their impact through daily viewing, the Claimant must have been aware that fraud can take place by someone purporting to call from the bank. The Respondent accepts that this was a sophisticated fraud, but equally it could easily have been stopped by abiding by the bank's simple advice. It is difficult to see what further training was required. The Claimant had primary responsibility for the company's online banking and had very recently engaged in a security review. Her oral evidence regarding the email of 10 April gave the impression that she did not take online banking security matters very seriously. She did not open either of the attachments and could not explain why. Had she heeded the advice, "beware of imposters", and recalled that the bank would never ask for digits from her password over the phone, alarm bells would have rung and the fraud would not have succeeded. It was not necessary for the bank or the Respondent to deliver specific training as to particular methods used by fraudsters and the Claimant has not identified any particular training that would have helped her.

39. The real dispute centres on whether dismissal was a reasonable sanction. The Claimant relies heavily on the fact that her conduct was not deliberate and the Respondent not having categorised her conduct as gross misconduct. The Respondent's witnesses accepted in cross-examination that the Claimant had not committed gross misconduct. The Claimant relied on the ACAS Code of Practice on Discipline and Grievance, which states that a final written warning is the most severe sanction that could be appropriate for a first instance of misconduct. She accepted, however, that the ACAS Code does not fetter the Tribunal's essential task in deciding whether dismissal fell within the range of reasonable responses.

I am satisfied that dismissal was a reasonable outcome in this case. I accept that 40. this was a sophisticated fraud and it is of course easier to see with hindsight where alarm bells should have rung, but the Respondent reasonably concluded that the Claimant's actions were so irresponsible that they could not continue to employ her. As noted above, it was naïve for the Claimant to assume that knowledge of a specific amount that was owed by a customer meant that it must have been a genuine call from the bank. She should have been alert to the fact that an incoming call from someone she had never spoken to before, requesting security details that would not normally be requested, might not be genuine. It was perhaps unlucky timing that "Andrew's" call was put through to the Claimant only 5 minutes after she had emailed Darren Clark, which might have contributed to her assumption that Andrew was "in the loop" with her correspondence with genuine NatWest employees. It was also perhaps understandable that the Claimant would place some reliance on the fact that the number Andrew appeared to be calling from was the same as the number given by Mohammed. None of that excuses the fundamental carelessness, however, in disclosing information that the bank itself had said would never be requested over the telephone. Particularly once the Claimant's card had been rejected, she ought to have realised that something was amiss. If she had been in any doubt, the sensible thing to do was put down the phone and call NatWest herself. I also consider it was not unreasonable for the Respondent to place some reliance on the Claimant's failure to accept responsibility. She claimed in her oral evidence that she apologised at the meeting on 23 May 2018, but this is not recorded in any of the documents and was not in her witness statement. The tenor of the arguments she was making throughout the disciplinary process was that she was the victim of a fraud for which she bore very little responsibility. It was not unreasonable for the Respondent to take the view that its trust in the Claimant was damaged beyond repair.

41. I do not place any significance on clause 22 of the handbook in assessing the reasonableness of the Respondent's conduct. The Claimant disputes that it applied to her, but it is so obvious that passwords etc. should be kept secure that it is irrelevant whether the handbook applied to the Claimant.

42. Gross misconduct is defined in the ACAS Code as conduct so serious in itself, or having such serious consequences, as to justify summary dismissal for a first offence. The Respondent has never said that the Claimant's conduct amounted to gross misconduct and it did not dismiss her summarily. She was paid in lieu of notice. As the EAT confirmed in *Quintiles Commercial UK Ltd v Barongo* [2018] UKEAT/0255/17 section 98(4) does not lay down any rule that dismissal will not be fair in cases falling short of gross misconduct. For the reasons given above I am satisfied that dismissal was a reasonable response to the Claimant's conduct.

43. The Claimant further argued that the disparity between the outcome in her case and that of Ms Thompson rendered her dismissal unfair. It has long been established that tribunals should take particular care when faced with arguments based on disparity. Guidance was given in *Hadjioannou v Coral Casinos Ltd* [1981] IRLR 352, the EAT setting out the circumstances in which disparity might be relevant to an unfair dismissal claim:

"Firstly, it may be relevant if there is evidence that employees have been led by an employer to believe that certain categories of conduct will be either overlooked, or at least will be not dealt with by the sanction of dismissal. Secondly, there may be cases in which evidence about decisions made in relation to other cases supports an inference that the purported reason stated by the employers is not the real or genuine reason for a dismissal. ... Thirdly ... evidence as to decisions made by an employer in truly parallel circumstances may be sufficient to support an argument, in a particular case, that it was not reasonable on the part of the employer to visit the particular employee's conduct with the penalty of dismissal and that some lesser penalty would have been appropriate in the circumstances." (para 24)

44. The EAT noted in the more recent case of *MBNA Ltd v Jones* [2015] UKEAT/0120/15 that the central question is whether it was reasonable for the employer to dismiss the employee whose case the tribunal is considering. "If it was reasonable for the employer to dismiss the employee whose case the ET is considering, the mere fact that the employer was unduly lenient to another employee is neither here nor there." (para 22)

45. I have already found that the decision to dismiss was reasonable. It was telling that the Claimant said during cross-examination that if Ms Thompson had been dismissed "we probably wouldn't be here". I do not accept the Claimant's argument that this case is in the rare category of cases where disparity led to unfairness. Ms Thompson's circumstances were not "truly parallel" to the Claimant's. The Claimant in fact seemed to maintain the argument that Ms Thompson's conduct was more serious because Mohammed had mentioned the possibility of fraud and she did not pass that on to the Claimant. It is true that at the time of disclosing the security details the Claimant was unaware of a possible fraud, whereas Ms Thompson was aware. That potentially made Ms Thompson's conduct more serious than the Claimant's, but it was mitigated by a number of factors. First, the number Ms Thompson had been given by Mohammed was displayed on the Claimant's phone. Secondly, Ms Thompson did not know that the Claimant was on an incoming call. Thirdly, she did not know that the Claimant was speaking to someone she had never spoken to before. Fourthly, the Claimant had primary responsibility for the relationship with NatWest and online banking, including security, and had given Ms Thompson the clear impression that the caller was bona fide. Although clearly Ms Thompson should not have disclosed the information, it was not unreasonable for the Respondent to conclude that she bore a lower level of responsibility for the fraud. It was also relevant that she had apologised.

46. As to the appeal, it was not good practice for Mr Dennison to consult Ms Thompson about the Claimant's appeal and to place weight on her views when she was so closely involved and had a vested interest in minimising her own culpability, but given that the original decision to dismiss was fair nothing turns on this point.

47. The Claimant has not raised any issues about the fairness of the procedure as a whole.

48. For the reasons given above the unfair dismissal complaint fails. It is therefore unnecessary to address the issues relevant to remedy.

Employment Judge Ferguson

Dated: 18 March 2019