WATRS

Water Redress Scheme

ADJUDICATOR'S FINAL DECISION SUMMARY

Adjudication Reference: WAT-X673

Date of Final Decision: 6 January 2022

Party Details

Customer:

Company:.

Complaint

The company received a fraudulent call regarding the customer's account and gave the fraudster the customer's email and home address. The company has failed to take responsibility for the data breach, even though the Information Commissioner's Office ("ICO") has confirmed it, or acknowledge the impact the situation has had on the customer. Therefore, the customer would like the company to provide her with a formal apology and £2,000.00 in compensation for distress and inconvenience.

Response

The General Data Protection Regulation (GDPR) does not give specific guidance on caller identity verification, but requires the company to take reasonable steps to secure and protect personal data from unauthorised release. On 19 August 2020, it received a fraudulent call about the customer's account, but the caller passed security by correctly providing the customer's name, address and date of birth, which enabled the call handler to proceed with the call believing that they were speaking to the customer. The call handler did not breach the GDPR, but the company apologises for any upset caused to the customer and has offered her £150.00 as a gesture of goodwill.

Findings

The evidence shows that the ICO has already investigated the customer's complaint and found that the company breached the GDPR. In view of this, Rule 3.5 of the WATRS Scheme Rules prohibits me from adjudicating on whether the company breached the GDPR. However, I am able to adjudicate on whether the company has failed to take responsibility for the breach found by the ICO, and whether it should apologise to the customer. The evidence

shows that the company has failed to accept that the ICO's investigation concluded that it had breached the GDPR. Therefore, I find that the company has failed to provide its service to the standard reasonably expected by the average person, and I direct the company to apologise to the customer and pay the customer £300.00 in compensation for the distress and inconvenience she has suffered.

Outcome

I direct the company to apologise to the customer for failing to accept responsibility for the GDPR breach investigated by the ICO, and for the negative impact this has had on the customer. I also direct the company to pay the customer £300.00 in compensation for distress and inconvenience.

ADJUDICATOR'S FINAL DECISION

Adjudication Reference: WAT-X673

Date of Final Decision: 6 January 2022

Case Outline

The customer's complaint is that:

- The company received a fraudulent call regarding her account, during which the company gave the fraudster her email address and her home address. She found out about this when she received emails about an online account she had not set up.
- When she reported the data breach to the company, she did not feel that it was taken seriously, so she raised it with the Information Commissioner's Office ("ICO").
- The company said that it was a fraudulent call and not a data breach, and as the fraudster already had some of her information, it believed that it was speaking to the correct person.
- The company would not give her a recording of the call as it did not have her voice on it, so she had to get a transcript of the call from the police.
- The company says it has taken steps to assist her; her account is now managed by one person and a note has been added to her account to say that she must be asked account specific questions rather than personal questions for security purposes. However, this was done at her request and was not offered by the company in order to help her.
- She remains unhappy as the ICO told her that the company would be in touch to offer its support, but it did not try to contact her, and when she contacted the company, she was made to feel like the issue was trivial and that the company was 'gas lighting' her. She was treated like a nuisance, not a customer with a valid complaint.
- The company has not taken responsibility for the situation, admitted there was a data breach, shown any compassion, or considered the impact this situation has had on her; even though the impact has been significant and she has had to change all her contact information and move house.
- In view of the company's failure to take responsibility, she would like the company to offer her a formal apology and pay her £2,000.00 in compensation for distress and inconvenience.

The company's response is that:

- Article 5 of the UK General Data Protection Regulations ("GDPR") sets out seven key principles which lie at the heart of data protection and require that personal data shall be:

  "(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

  (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

  (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

  (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

  (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

  (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

- The GDPR does not give specific guidance on caller identity verification, but it requires that personal data handling should comply with the seven key principles. It believes that the most relevant of the seven key principles is (f) 'integrity and confidentiality', which means that it must take reasonable steps to secure and protect personal data from unauthorised release.
- On 19 August 2020, it received a fraudulent call about the customer's account. The caller passed security by correctly providing the customer's name, address and date of birth, which enabled the call handler to proceed with the call believing that they were speaking to the customer. During the call, the caller stated that they could not provide their telephone number as they were dyslexic. This was not challenged by the call handler as they did not want to discriminate against this. However, the caller was asked, "You rent the property, don't you

Rachel?" and the caller answered correctly. As a result of the call, an online account was set up, but the call handler did not provide a password. No data breach occurred during this call.

- The customer asked for a recording or a transcript of the call, but it was unable to provide this as the call was not made by the customer. Therefore, it passed the recording on to the police and the police were able to provide this to the customer.
- As set out in its correspondence with the ICO, it has taken further steps to reinforce awareness training for its agents, and its post-call survey now asks customers who have not made contact prior to receiving the survey to make immediate contact. It has also added the customer's name to the Priority Services Register to ensure a small team manage her account, and changed the identity verification questions on the customer's account so that she is only asked information about her account, rather than her personal details, in the future.
- The customer believes there was a data breach and wants it to apologise and accept responsibility for this. Although it does not accept that there was a data breach, it has apologised to the customer on a number of occasions for the upset she has suffered as a result of the fraudulent telephone call.
- On 14 May 2021, it offered the customer £100.00 as a gesture of goodwill in apology for the distress and upset the customer has suffered, but this was not accepted. On 22 July 2021, it increased this offer to £150.00 in its response to the CCW Pre-investigation, but, again, this offer was not accepted. The offer remains open should the customer now wish to accept it.
- It would like to say sorry to the customer again and reiterates that it fully acknowledges the upset this situation has caused her, but denies responsibility to provide a formal apology.

How is a WATRS decision reached?

In reaching my decision, I have considered two key issues. These are:

1. Whether the company failed to provide its services to the customer to the standard to be reasonably expected by the average person.
2. Whether or not the customer has suffered any financial loss or other disadvantage as a result of a failing by the company.

In order for the customer's claim against the company to succeed, the evidence available to the adjudicator must show on a balance of probabilities that the company has failed to provide its services to the standard one would reasonably expect and that as a result of this failure the customer has suffered some loss or detriment. If no such failure or loss is shown, the company will not be liable.

I have carefully considered all of the evidence provided. If I have not referred to a particular document or matter specifically, this does not mean that I have not considered it in reaching my decision.

How was this decision reached?

1. The customer claims that the company breached the GDPR during a fraudulent telephone call made on 19 August 2020, and says that she referred her complaint to the ICO and the breach was confirmed. The customer wants the company to apologise for failing to take responsibility for the breach of the GDPR and for failing to consider the impact the breach has had on her. The company states that it did not breach the GDPR and the ICO decided not to take any further action after its investigation.

2. The evidence I have been provided with includes an email from the ICO to the company, dated 17 February 2021, which states, "We would like to understand if you have identified the reason the data was breached and what safeguards are in place to help ensure you handle personal data properly, particularly in relation to this specific matter." The evidence also includes an email sent to the customer from the ICO, dated 19 March 2021, which states, "I have considered the information available in relation to this complaint and I am of the view that X Limited have infringed the general data protection regulations."

3. In view of this evidence, I accept that the ICO investigated whether the company breached the GDPR and concluded that it had.

4. As the breach of the GDPR has already been investigated by the ICO, I consulted the WATRS Scheme Rules to establish whether I am able to adjudicate on this matter.

5. Rule 3.5 of the WATRS Scheme Rules states:

   "The Scheme cannot be used to adjudicate disputes which fall into one or more of the following categories:

   - disputes concerning the Competition Acts 1998 and 2002 as amended;
   - regulatory enforcement cases;
   - bulk supply determinations;
   - disputes between undertakers, between licensees and between undertakers and licensees;
   - water supply licensing disputes;

- whistle blowing;
- any matters over which Ofwat has powers to determine an outcome
- disputes relating to eligibility to transfer to a statutory licensee;
- water quality legal standards;
- enforcement cases under the Environmental Protection Act 1990 and the Environmental Act 1995 as amended;
- disputes that are subject to existing court action or on which a court has ruled unless the court's decision has been set aside;
- disputes that are the subject of an existing or previous valid application under the scheme;
- the handling of CCWater and Ofwat complaints;
- complaints which are being or have been investigated by a statutory or regulatory agency or agencies including the Drinking Water Inspectorate and/or the Environmental Agency in respect of the breach of a statutory or regulatory requirement unless a WATRS Notification or Option Letter has been issued in respect of the complaint;
- resale and third party complaints;
- disputes relating to the fairness of contract terms and/or commercial practices;
- disputes concerning allegations of fraudulent or criminal activity; and
- any dispute or disputes that are considered by WATRS to be frivolous and/or vexatious."

6. In view of Rule 3.5, I find that this Scheme cannot be used to adjudicate on whether the company breached the GDPR during the fraudulent telephone call of 19 August 2020. This is because the ICO is a regulatory agency and it has already carried out an investigation in respect of whether the company has breached a statutory or regulatory requirement (the GDPR). I appreciate that the customer may be frustrated by this, but, unfortunately, I do not have the jurisdiction to consider this matter.

7. As Rule 3.5 prohibits me from adjudicating on whether the company breached the GDPR, I cannot direct the company to apologise to the customer for any breaches. However, on the customer's application for adjudication, she states that she wants the company to apologise because "they have not accepted responsibility" or "considered how this has impacted her", and I find that I am able to consider whether the company should apologise to the customer for failing to take responsibility for the breach found by the ICO, and failing to consider how the breach found by the ICO impacted her.

8. The evidence shows that the company has repeatedly apologised for the upset this situation has caused the customer, but the apologies have fallen short of accepting that a data breach occurred, and the company has not acknowledged that the upset caused to the customer was due to an actual breach of GDPR, rather than her mistaken belief that a breach had occurred. Also, the company's response to the customer's claim confirms that it does not accept that the conclusion of the ICO's investigation was that it had breached the GDPR.

9. In view of this, I find that the company has failed to provide its service to the standard reasonably expected by the average customer. I therefore direct the company to apologise to the customer for failing to accept responsibility for the GDPR breach investigated by the ICO, and for the negative impact this has had on the customer.

10. Following the preliminary decision, the company submitted comments disputing that it has failed to accept the outcome of the ICO's investigation. The company states that the ICO's letter to the customer states that the company has reviewed its processes and outlines the actions the company agreed to take in response to the investigation, and the agreed actions show its commitment to improving its service. The company also reiterates that the ICO concluded that no further action was needed and no breach of GDPR occurred.

11. However, while I accept that the company agreed to undertake certain actions in response to the ICO's involvement, and the ICO decided no further action was necessary, my view remains that the letters from the ICO show, on the balance of probabilities, that the outcome of its investigation was that the company breached the GDPR during the fraudulent telephone call. Furthermore, while the company provided comments on the preliminary decision, it has not provided any further evidence, such as correspondence from the ICO, to undermine my preliminary findings.

12. Further, the company's comments in its response document, coupled with its comments on the preliminary decision, confirm that the company does not accept that a GDPR breach occurred. For example, the company states, "REDACTED have apologised to Miss Rachel Scarrott for the upset & inconvenience this may have caused her but do not accept a GDPR breach took place", "REDACTED have maintained the approach that during this call no data breach occurred", and "on review

    REDACTED believe that the amount offered in the response to CCW is fair considering that REDACTED have not breached any GDPR." Therefore, despite agreeing actions with the ICO, my decision

remains unchanged and I find that, on the balance of probabilities, the company has failed to acknowledge to the customer that a GDPR breach occurred and the company should apologise to the customer for this.

13. Following the preliminary decision, the customer also provided comments and it came to light that as a result of an administrative error, her claim for compensation for distress and inconvenience had been left off her application form. In view of this, it is appropriate for me to consider the customer's claim for compensation now.

14. As stated above, Rule 3.5 of the WATRS Scheme Rules means that I am unable to adjudicate on whether the company breached the GDPR, as this has already been considered by the ICO. The Scheme Rules also mean that I am unable to direct the company to pay compensation for the breach of the GDPR investigated by the ICO. I understand that the customer will be extremely disappointed by this, but, as an adjudicator operating under the WATRS Scheme Rules, I have no authority to direct the company to provide a remedy for matters I am unable to adjudicate on. However, I am able to consider awarding compensation for the distress and inconvenience suffered by the customer as a result of the company's failure to accept the outcome of the ICO's investigation.

15. The customer explains that the company's failure to accept the ICO's decision has caused her considerable distress and anxiety. The customer describes the last fifteen months as 'horrific' because the company decided to 'fight' her and 'lie' to her, rather than own its failings and support her. The customer explains that the situation has had an impact on her physical and mental health, she has lost some of her hair, and she has struggled with suicidal thoughts because of the way she has been treated. It is difficult to distinguish the impact of the data breach from the impact of the company's refusal to accept there was one and, as explained, I can only direct the company to pay compensation for the latter, however, having considered the information provided by the customer, I fully accept that the company's failure to accept the decision by the ICO contributed considerably to the high level of distress and frustration the customer has suffered.

16. In order to assess the customer's claim for compensation, I looked at the WATRS Guide to Compensation for Distress and Inconvenience. Having considered all the circumstances of the case, I find that the customer's claim falls into the middle range of the 'Tier 2' category on the

award scale and, therefore, I direct the company to pay the customer £300.00. I understand that this is less than the amount claimed and the customer may be disappointed, however, I find this a reasonable amount of compensation for the company to pay for the failings shown in evidence and for which I have the authority to adjudicate on.

Outcome

I direct the company to apologise to the customer for failing to accept responsibility for the GDPR breach investigated by the ICO, and for the negative impact this has had on the customer. I also direct the company to pay the customer £300.00 in compensation for distress and inconvenience.

What happens next?

- This adjudication decision is final and cannot be appealed or amended.
- The customer must reply by 20 January 2022 to accept or reject this decision.
- When you tell WATRS that you accept or reject the decision, the company will be notified of this. The case will then be closed.
- If you do not tell WATRS that you accept or reject the decision, this will be taken to be a rejection of the decision.

K S Wilks

Katharine Wilks

Adjudicator