EDR Response Guide – Disputed transactions (including remote access)

This guide has been prepared to assist financial firms in preparing a quality external dispute resolution (EDR) response for complaints about a chargeback by a complainant. This is a **guide only**.

It is important to note the following:

* All issues raised in a complaint should be addressed. If there are multiple issues, please refer to the additional EDR response templates available or consider addressing them in a separate section as it is important that all issues are addressed.
* This is your EDR response. As such it is to be sent to both AFCA and the complainant. It is to the benefit of all parties for the complainant to understand the reason for your position.
* AFCA will generally seek more information if a complaint does not resolve at Registration & Referral. AFCA still expects a response to any subsequent requests for information.

This guide may change over the time to reflect any feedback.

To ensure a comprehensive response for complainant chargeback complaints, an EDR response should include the sections outlined below.

## Complaint details

* Name of the complainant(s): [consumer or business name]
* Name of the financial firm:
* Financial firm reference:
* AFCA reference:

## Standard information request – disputed transactions

This information request applies to cases where the complainant disputes making, or otherwise authorising, a transaction (or series of transactions) from their account(s). Complaints raising disputed transactions may occur in the context of scams (such as remote access scams).

Where AFCA is satisfied the disputed transaction(s) are unauthorised, AFCA will investigate how liability should be approached in accordance with the ePayments Code. If the financial firm is not a subscriber to the ePayments Code, AFCA will assess liability based on the terms and conditions applicable to the account.

1. Please confirm the bank’s understanding of the complaint and the bank’s position on the issues raised.
2. For each transaction the complainant disputes, please provide a table setting out the:
	* transaction date, value and recipient
	* transaction method (e.g. internet banking, BPay, card payment, etc).
3. Please provide copies of all supporting documentation, including:
	* all correspondence, contact notes, diary notes and call recordings with the complainant in relation to the disputed transactions
	* relevant terms and conditions of the account and internet banking service
	* statements for all accounts the complainant held with the bank from three months prior to the first disputed transaction, to present
	* any responses to the complainant.
4. Please provide a brief timeline of events in relation to the disputed transaction(s), including when the complainant first disputed the transactions with the bank, along with any supporting documents.
5. Please provide a detailed internet banking log from three months prior to the first disputed transaction until the current date. The log should include:
	* details of the transactions made on the complainant’s accounts via internet banking (both those that are in dispute, together with undisputed internet banking transactions during the same period)
	* activity on the complainant’s account, including all SMSs, on-screen warnings or codes sent to the complainant’s mobile phone or device
	* IP addresses indicating the location of where the transactions took place and which access method was used, such as mobile app or internet banking via an internet browser
	* any changes made to the complainant’s internet banking profile, such as daily transfer limits or contact details.
6. Please provide the wording of any SMSs/on-screen warnings identified above.
7. If the disputed transactions were conducted with a card and PIN:
	* if/when the complainant reported the card lost or stolen
	* date the card was issued
	* date the PIN was set
	* whether the PIN was system generated or self-selected
	* if self-selected, the date of the last PIN change.
8. If the bank’s position is that the complainant breached the passcode security requirements under clause 12 of the ePayments Code, please provide:
	* information to show the information the bank provided to the complainant regarding passcode security under clause 8 of the ePayments Code
	* information and documents (to the extent not already provided) to support the bank’s position that the complainant breached the passcode security requirements.
9. Is the bank willing to make any offers in resolution of this complaint? If yes, please provide details of the bank’s offer.

## Additional questions for remote access scam complaints

1. When did the complainant first contact the bank about the scam? Please provide supporting information.
2. The complainant says the bank should have been aware they were being scammed and acted to prevent the transactions. Please comment on this and provide any information to support the bank’s position.
3. Did the complainant have any interactions with the bank at the time the transactions occurred, including over the phone or in branch?
	* For any phone interactions, please provide a copy of the call recording(s)
	* For any branch interactions, please provide a statement from the branch manager and/or any staff members who dealt with the complainant during their visit to the branch setting out their recollection of the interaction.
4. A chronology of events, detailing the bank’s efforts to recall the funds (including follow up), including all responses and documents received from the receiving bank. Did the receiving bank confirm the funds were withdrawn in their entirety? If so, when?
5. If any of the disputed transactions were card transactions, please provide information to show how the bank met its chargeback obligations under the [**Banking Code of Practice**](https://www.ausbanking.org.au/banking-code/) or [**Customer Owned Banking Associate Code of Practice**](https://www.customerownedbanking.asn.au/how-it-works/code-of-practice):
	* what chargebacks were attempted
	* if no chargeback attempts were raised, please explain why?
	* if chargebacks were raised, what chargeback code was used and for what reason?
	* provide a copy of the bank’s complete chargeback file and a copy of all documentation showing its chargeback attempts
	* outline the chargeback reason for the transactions in reference to the scheme rules. Copy of all correspondence sent to and received from the institution that received the disputed transaction(s).
	* AFCA has published a [Chargeback Factsheet](https://www.afca.org.au/about-afca/publications/factsheet-chargebacks) which provides more information about chargeback obligations.

## Additional information requested for information/documents subject to a non-exchange request

Generally, AFCA cannot rely upon information when reaching a decision that has not been shared with the other party(s) to a complaint, unless special circumstances apply. This is in line with sections A.10.4 and A.10.5 of our Rules, which you can find [**here**](https://www.afca.org.au/about-afca/rules-and-guidelines).

For us to assess whether special circumstances apply, please provide the following information in relation to any information the bank requests not to be exchanged:

1. Which part(s), of the document(s) are you concerned about? Please be specific.
2. What are the reasons for your concern? Where possible, provide supporting information.
3. Why should AFCA take the information into account without exchanging it? Explain why the information is significant.
4. Suggest ways in which you might be able to provide the information in an alternative format so that the other party can see and respond to it. For example, you may be able to block out a witness’s name and details, but still leave the majority of the information intact.

## Jurisdictional issues?

Include the details of any jurisdictional issues the financial firm wishes to raise. Ensure you refer to the AFCA Operational Guidelines and any relevant approach documents.

Full details of the section of the AFCA Rules must be included to ensure that AFCA and the complainant understand the jurisdictional issue(s) being raised.

## Other issues raised?

If other issues are raised, we offer a range of resources in the member resources section of the Secure Services portal. These include other EDR response guides, specific complaint topic guides and the Complaint Information Documentation guide.