


## Security Check

This procedure guides you through performing a telephone security check when a client or a client representative contacts the Child Maintenance Group (CMG) or when the CMG contacts a client or client representative. Confirm the identity of a caller before divulging any confidential information. Any bogus calls must be documented and sent to the Security Advice and Support Centre.

The process is applicable to every phone call that a caseworker has with a client or client representative at any point during a case, for all inbound and outbound calls.

Check the client's answers against those recorded on the system and take any necessary action if the client fails security validation. Every client has chosen a seven digit personal identification number (PIN) and a special customer password during the application stage. Client representatives have their own SCIN, PIN, special customer password recorded when their details are added to the system.

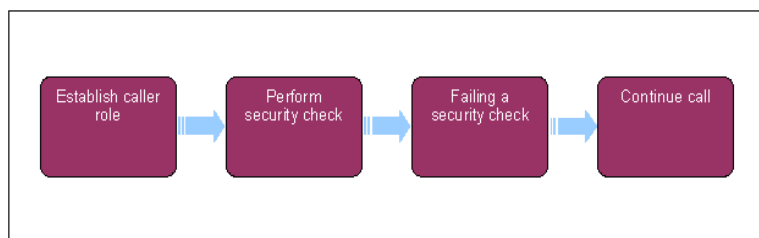
When the caller has failed a security check and the caseworker believes the caller is not a client/client representative, terminate the call and complete a [Bogus Call Report Form](#).

 No security check is required for an outbound call to employers/agents. When CMG contacts an employer/agent they are only required to confirm the organisation and that they are speaking to the payroll department.

For information on how to answer a call and speak to a client refer to [Call - Overview](#).


A desk aid has been created to help caseworkers and is available here: [Security Desk Aid](#).


For more information refer to the Policy, Law and Decision Making Guidance .



 When speaking to clients always use the new terminology. For more information refer to [Terminology Changes](#).


### Establish caller role

-  The security check is similar whether on an inbound or an outbound call. Establish whether you are speaking to a client or a client representative. Client representatives have their own SCIN, PIN, special customer password recorded when their details are added to the system. They should use these when calling in regarding a client case.
- If the person you are talking to is a client or a client representative, continue with the security check.

 If the person is not the client or a registered client representative, or the representative is calling in using the client SCIN, the client must be present to go through the security process. The client must grant permission for their representative to continue the phone call. If the client is not present to go through the security process, explain that, due to data protection restrictions you must end the call. Record the call outcome and establish caller role.

### Perform Security Check


-  For guidance on Third Party organisations where security has not been set up, refer to [Third Party - Contact](#).


 If the Initial Calculation has been completed, or the case has recently gone through transition from 1993/2003 scheme without contact being made, (also if the provisional/indicative calc has been completed and it is our first contact with the paying parent), the security details may show as **Apply Defaults** or today's date and the PIN as 1234567. In this event ask the caller to confirm their identity by using the information already held by CMG: Transitional Security Questions:


- Postcode
- Date of Birth
- QC Date of Birth
- SCIN


- NINO

Ask the caller to confirm at least three of these in order to ensure you are speaking to the correct person. Once the identity of the caller has been established, collect the required security details. For more information refer to [Security - Set Up](#).

 If the case is arrears only transitioned cases, QC DOB should not to be used as one of the security check questions as this has been defaulted for these cases.

-  The caller details show in the **Contact Summary** screen, along with the security details. Select the **Get Security Questions and Answers** tab; two random digits from the PIN, the special customer password and two randomly selected security questions are displayed in this field.

 If the case was active prior to 22/8/2016 the system will have information in the memorable questions fields. When Get Security questions and answers is selected it also generates 2 randomly security questions from the 7 memorable questions. Caseworkers should ignore this information as it is no longer required as part of the security process.

 **Never** disclose the personal information (please also see [Protecting Client Information](#)) we hold - even once Security has been passed. If a client provides their details, address, etc, thank them for the information but **do not volunteer** the following information:

- Date of Birth
- National Insurance Number
- Bank or Building Society data (however the last 4 digits are acceptable)
- Full telephone number (however the last 4 digits are acceptable)
- Client's email addresses
- Current address
- Details of appointees

### Inbound call

- If the call is inbound, perform the security checks as detailed in the table below. You must ensure that you request the pin digits one number at a time and a response has been provided before asking for the next digit.


Two PIN digits correct? (Request twice if incorrect first time before asking any other security questions)	Special customer password correct?	One Transactional/Transitional Security question correct?	Outcome
Yes	Yes	Not Required	Security passed, go to step 19
Yes	No	Yes	Security passed, go to step 6 then step 19
Yes	No	No	Failed - go to step 8
No	Yes	Yes	Security passed, go to step 6 then step 19
No	Yes	No	Failed - go to step 8
No	No	Not Required	Failed - go to step 8


- Customer record must be updated to note additional question used due to PIN/Password failure. Create an **Activity – Record** at contact level using a future start date of 01/01/2035 and add a note within the description field and set the activity **Status to Not Required**. This activity will always appear at the top of the activities tab making it easy for caseworkers to identify if additional security has previously been used.

 Clients to be reminded that future contact will require correct PIN/Password before progressing the call.

- Should the customer on future contact fail either PIN/Password then a full reset must be undertaken. Use of transactional/transitional questions should not be pursued. If this occurs again a re-set should be completed. If a re-set is completed update the description field to note this to prevent security being re-set un-necessarily.

- Inform the client if they have not successfully answered the security questions. Offer to call the client back to ask 3 additional transactional questions on the case to validate their identity. If the client accepts this, continue to the next step, if the client refuses, go to **step 16**. If you are a General Inbound Call Handling (GICH) team member, advise the client you will arrange for the caseworker dealing with the case to call them back.

 When answering an inbound call and entering the client's ID, an error message may display which prevents security validations from being completed on the system. On receipt of an error message, offer to call the client back in order to ask the security questions to validate their identity.

 If the caller fails security, do not confirm the telephone number held on the system. Advise the client you will call them back on the number held on the system. A call back will be arranged for the caseworker to complete. If there is no number held on the system or if the number held is unobtainable caseworker to access CIS and CRA to trace an up to date telephone number. For more information on using these trace tools see [Confirm Current Location](#).

9. Call the client back, ask three of the following transactional questions for them to confirm their identity:

- Date of Birth of one QC
- Name of current/previous employer
- Method of payments usually made/received
- Last 4 digits of client bank account
- What was last contact about
- First name of other person in the case (receiving parent/paying parent)

Ask transactional questions where possible, but if the case is at an early stage of the lifecycle, (meaning the client may be unable to answer three transactional questions regarding their case), and ask the caller to confirm at least three of the details already held by CMG -**Transitional questions**.

- Postcode
- Date of Birth
- QC Date of Birth
- SCIN
- NINO

10. If the client correctly answers the questions, thank them for completing the security check then reset their security details, for more information refer to [Change - Security Details](#). Advise them of the importance of remembering their unique PIN (as the system only allows three failed PIN attempts before the account is blocked) and password. Go to **step 17**.

11. If the client answers any of the questions incorrectly, inform them they have failed the security check and you cannot continue with the call. Go to **step 16**.

### Outbound call

12. If the call is outbound, perform the security checks as detailed in the table below. Ensure that you request the pin digits one number at a time and that a response has been provided before asking for the next digit.

Two PIN digits correct? (Request twice if incorrect first time before asking any other security questions)	Special customer password correct?	One Transactional/Transitional Security question correct?	Outcome
Yes	Yes	Not Required	Security passed go to then step 19
Yes	No	Yes	Security passed go to step 6 then step 19
Yes	No	No	Failed - go to step 13
No	Yes	Yes	Security passed go to step 6 then step 19
No	Yes	No	Failed - go to step 13
No	No	Not Required	Failed - go to step 13


13. Inform the client they have failed the security check and ask three of the following transactional questions for them to confirm their identity:


- Date of Birth of one QC
- Name of current/previous employer
- Method of payments usually made/received
- Last 4 digits of client bank account
- What was last contact about
- First name of other person in the case (receiving parent/paying parent)

Ask transactional questions where possible, but if the case is at an early stage of the lifecycle, (meaning the client may be unable to answer three transactional questions regarding their case), and ask the caller to confirm at least three of the details already held by CMG - **Transitional Security**.


14. If the client correctly answers the questions, thank them for completing the security check then reset their security details, for more information refer to [Change - Security details](#). Advise them of the importance of remembering their unique PIN (as the system only allows 3 failed PIN attempts before the account is blocked) and password. Go to **step 17**.
15. If the client answers any of the questions incorrectly, inform them they have failed the security check and you cannot continue with the call. Go to **step 16**.

## Failing a security check

16. End the call and record the outcome as **Failed ID Security Check**.
17.  Where there have been three separate consecutive calls and failed security checks, the client or client representative is blocked on the system. Call the client and ask their customer password/PIN or three transactional questions as above to allow you to unblock the clients account. If the client passes the security check, unblock their account, for more information refer to [Change - Security Details](#).  
If the client fails the security check again or you cannot contact them by phone, issue CMSL9800 'We need to update your security details' and FT9800 to the address we hold on the system for the caller. If the client or client representative has not responded to the letter and form after seven days, consider sending an SMS . Refer to [SMS Text](#) for further information. If an SMS text message is not appropriate, issue reminder letter CMSL9801 'Reminder - We need to update your security details'.



 When issuing the letter, if the case is still at the application stage, set the wait activity to **Not Required**. (If this is set to **Done** the system closes the case after the wait period).

18. The client remains blocked and will not be able to discuss their case by telephone until their security details are successfully updated. To unblock a client's account refer to [Change - Security Details](#).  
If the client does not respond to CMSL9801 record this in Notes. Update the SR Sub Status to CoC Decline then update the activity plan Outcome to CoC Declined. Change the Resolution Code to CoC Rejected and close the SR.

 If you believe this is a bogus call, document the call and send the information to the Security Advice and Support Centre flagging this as a priority, if it is the third consecutive failed call complete the bogus caller form. When completing the form use the Features of call/Further details section to record the scheme client identification number (SCIN) of the contact you were trying to call.

To contact the Security Advice and Support Centre and access the form select the following link:

[Security Advice and Support Centre](#)

 For more information on bogus calls refer to the Policy, Law and Decision Making Guidance 

## Continue Call

19. Once you are certain of the caller's identity and role in the case, continue with the call. Establish the reason for the call, and continue accordingly. For more information refer to [Call - Overview](#).
20. When a call is transferred after a successful security check, no further check is needed following the warm hand-on.

### CMSL9800 We need to update your security details

Failed security details - client has failed their security check and we enclose a change to security details form.  
All fields in this letter are system generated, no manual intervention is required.

### CMSL9801 Reminder - we need to update your security details

After client fails their security details, we send them a form to update their security details. This is a reminder letter – sent after 7 days to remind the client to fill in the form or they won't be able to speak to the CMG about their case.  
All fields in this letter are system generated, no manual intervention is required.

[Call - Overview](#)

[Change - Contact Details](#)

[Change - Security Details](#)

[Incident Management - Manage Incident Locally](#)

[Security - Set Up](#)

[Terminology Changes](#)

[Third Party - Contact](#)

