Home Office

Passport cancellations: malicious lost and stolen reports

Version 4.0

This guidance tells His Majesty's Passport Office staff how to deal with malicious lost and stolen passport reports.

Contents

About: Passport cancellations: malicious lost and stolen reports

This guidance tells His Majesty's Passport Office staff how to deal with customer queries, when a malicious lost and stolen report has resulted in the cancellation of a passport (from a loss report).

Contacts

If you have any questions about the guidance and your line manager or senior caseworker cannot help you or you think that the guidance has factual errors then email Guidance & Quality, Operating Standards

If you notice any formatting errors in this guidance (broken links, spelling mistakes and so on) or have any comments about the layout or navigability of the guidance then you can email Guidance & Quality, Operating Standards.

Publication

Below is information on when this version of the guidance was published:

- version **4.0**
- published for Home Office staff on **28 September 2022**

Changes from last version of this guidance

This guidance has been updated to reflect the change in our sovereign from Her Majesty Queen Elizabeth II to His Majesty King Charles III.

Related content
Contents

Malicious lost and stolen reports

This section tells HM Passport Office staff, what a lost and stolen report is and includes what malicious lost and stolen reports are, how we might receive one and how to deal with it.

When a customer declares their passport as lost or stolen, HM Passport Office will electronically cancel it in our records.

The Lost, Stolen and Recovered (LSR) team or Sopra Steria Ltd (SSL) create and process lost or stolen records based on information that a passport holder or third party gave them. They get this information:

- on a paper LS01 form
- on a Digital Lost and Stolen (DLSR) report from GOV.UK
- by phone
- from trusted sources, such as the Foreign Commonwealth and Development Office (FCDO)

What a malicious report is

A person may falsely, fraudulently or dishonestly declare another person's passport as lost or stolen for malicious reasons. These include but are not limited to:

- stopping a person from traveling
- inconveniencing a person
- causing them harm
- parental or child disputes

If the person provides all of the information we need to process an LSR report on:

- an adult passport, we will:
  - cancel the passport and record it as 'lost' or 'stolen' on Main Index
  - not carry out further checks
- a child passport, we will:
  - confirm that the person reporting the cancellation is the person who originally applied for the child passport
  - carry out further checks before deciding if the passport should be cancelled (in line with the LSR examiner guidance)

If a third party made the LSR report maliciously, the passport holder may not be aware.

How malicious LS reports are identified

The passport holder may find out that their passport has been electronically cancelled and a lost and stolen (LS) record created when they:

- are using the passport for travel (during Border Force, or overseas immigration checks when the customer tries to leave or enter the UK)
- are using the passport for identity checks (if the check includes passport validation, and a data verification (DVA) check)
- receive a DLSR notification by email

HM Passport Office may become aware of a malicious report when:

- the customer contacts us (by phone, email, or by attending a passport office) asking why:
  - their passport is cancelled (for example, if Border Force have told the customer that their passport has been cancelled)
  - they have received a DLSR notification
  - we have issued a new passport, when they still have a current valid passport
- the customer tells us they have not declared their passport lost, when:
  - SSL contacts them about a DLSR report they are processing
  - an examiner contacts them if they are processing an application

Related content
Contents

Examiners dealing with malicious LS reports

This section tells HM Passport Office examiners how to deal with passport applications when customers tell us about a malicious passport cancellation report.

You, the passport examiner, may become aware of a malicious lost and stolen (LS) report when processing an application, if:

- you contact the customer about their application and they tell you they did not cancel their previous passport
- the customer provides a covering letter to state their new application is to replace a passport that was previously cancelled by someone else

Customer makes us aware of a malicious LS report

If the customer makes you aware of a malicious LS report when dealing with their application, you must:

1. Phone the customer and ask them for the folllowing details, including:
   - full name
   - date of birth
   - place of birth
   - contact telephone number
   - contact address
   - email address
   - passport number (if known)
2. Search Main Index (MI) for lost and stolen records (LSR) using the customer's details to find the loss report.
3. Check the reason for cancellation, and who reported the loss.
4. Check to see if any further passports have been issued.

Then, you must decide if:

- the LS report was made maliciously or using false, dishonest, or fraudulent information
- the LS report was not malicious, for example:
  - HM Passport Office cancelled the passport in error
  - the customer did report the loss but they had forgotten
  - the customer had travelled using the wrong passport (previously reported as lost)

Examiner decides LS report was made maliciously

If you decide the previous passport has been cancelled due to a malicious LS report, you must:

1. Ask the customer if they have already reported the false report to the police.
2. Send an email to the Intel Hub, and copy in Passport Service Management Team (PSMT). This email must include:
    - full name
    - date of birth
    - place of birth
    - contact telephone number
    - contact address
    - email address
    - details of the malicious LS report, including details of the cancelled passport
    - name of the police force where the report has been made (if the false report has been already reported to the police)
    - the crime reference number (if the false report has been already reported to the police)

If the customer has not made a report to the police, you must tell the customer we must report the malicious LS report to the police. The Intel Hub will report the malicious LS report to the police as part of their process when they action the referral.

If you have any safeguarding concerns (for example, a child application where there are signs of a parental dispute), you must not continue to process the application. You must refer the application to Intel Hub, who will liaise with Child Protection and Safeguarding team (CPST).

If you have no safeguarding or fraud concerns, you must continue to process the application in line with the relevant guidance.

Where a malicious LS report has been identified, a replacement passport will be issued to the customer free of charge (gratis). This passport must be valid until the expiry date of the cancelled passport. You must give the customer the choice of:

- a full refund for the application they have made, but we issue their new passport with the remaining validity of their cancelled one
- a full validity passport, but we retain the fee they have already paid

You must tell the customer to return their cancelled passport to us if they still hold it, in line with the LSR guidance.

Examiner decides LS report was not malicious

If you decide that the report was not malicious, you must tell the customer:

- we have investigated the report
- we are satisfied there are no concerns or discrepancies
- we will not be taking any further action

You must then continue to process the application in line with the relevant guidance.

If a customer wants to make a complaint

If customer wants to make a complaint you must follow the complaints procedure.

Related content
Contents

CSMT: dealing with malicious LS reports

This section tells HM Passport Office Customer Service Management team how to deal with customers who ask why we have cancelled their passport or tell us they, have not reported the passport lost or believe someone has maliciously cancelled their passport.

You, the Customer Service Management team (CSMT) staff member, can get potential malicious reports from:

- the customer, by phone or email
- staff in an Application Processing Centre (APC), for example, if the customer visits a passport office asking why their passport has been cancelled
- staff on the Passport Service Management team (PSMT), when cases are referred from:
  - Sopra Steria Ltd (SSL)
  - Lost, Stolen and Recovered (LSR) team
  - Disclosure team
- The Foreign, Commonwealth & Development Office (FCDO), where a customer is overseas

The customer may:

- know or believe the loss was reported maliciously
- have reported the malicious report and false declaration to the police
- have received a ‘non-disclosure’ letter from the Disclosures team
- not be aware why their passport has been cancelled
- be aware of a dispute between the parents of a child, leading to a passport being cancelled maliciously

You must investigate the customer’s query and the LSR report to decide if the report is malicious. The report may be malicious if, for example, the customer states that they have not cancelled the passport.

Where a malicious report has been identified, a replacement passport will be issued to the customer free of charge (gratis). This passport must be valid until the expiry date of the cancelled passport.

If the customer is overseas and a malicious report has been identified, you must tell them to:

1. Contact the FCDO.
2. Request an Emergency Travel Document (ETD) if they need to travel urgently.
3. Continue to provide the customer with a free of charge (gratis) passport, valid until the expiry date of their cancelled passport.

How CSMT identify a malicious report

When you are checking an LSR report to decide if it is malicious, you, the Customer Service team (CSMT) must ask the customer for their details, including:

- full name
- date of birth
- place of birth
- contact telephone number
- contact address
- email address
- passport number

You must:

1. Search Main Index (MI) for lost and stolen records (LSR) using the customer's details to find the loss report.
2. Check the reason for cancellation, and who reported the loss.
3. Check to see if any further passports have been issued.

Then you must decide if:

- the LSR report was made maliciously or using false, dishonest or fraudulent information
- the LSR report was not malicious, for example:
  - HM Passport Office cancelled the passport in error
  - the customer did report the loss but they had forgotten
  - the customer had travelled using the wrong passport (previously reported as lost)

CSMT confirms LS report was malicious

If you decide the passport has been cancelled due to a malicious LSR report, you must ask the customer if they have already reported the false report to the police.

Customer already informed the police

If the customer has already reported the LSR report to the police, you must:

1. Ask for the details of the police report, including the:
   - name of the police force where the report has been made
   - crime reference number
2. Tell the customer to send us a new passport application with a letter explaining about the malicious report and include the crime number from the police.
3. Send an email to the Intel Hub, and copy in PSMT. This email must include:
   - full name
   - date of birth
   - place of birth

    - contact telephone number
    - contact address
    - email address
    - details of the malicious report, including details of the cancelled passport
    - details of the police report
4. Add the customer's details to the Customer assurance complaint log as a malicious report case.

You must tell the customer to return their cancelled passport to us if they still hold it, in line with the LSR guidance.

Customer has not informed the police

If the customer has not made a report to the police, you must:

1. Tell the customer we must report the malicious report to the police.
2. Send an email to the Intel Hub, and copy in PSMT. This email must include:
    - full name
    - date of birth
    - place of birth
    - contact telephone number
    - contact address
    - email address
    - details of the malicious report, including details of the cancelled passport
3. Add the customer's details to the Customer assurance complaint log as a malicious report case.

You must tell the customer to return their cancelled passport to us if they still hold it, in line with the LSR guidance.

CSMT decides the LS report was not malicious

If you decide that the report was not malicious, you must tell the customer:

- we have investigated the report
- we are satisfied that they have sent it and there are no concerns or discrepancies
- we will not be taking any further action
- to apply for a replacement passport if they need one (they must pay the full fee for that replacement passport application)

If the customer is overseas, you must tell them to contact the Foreign, Commonwealth & Development Office (FCDO) and request an Emergency Travel Document (ETD) if there is an immediate need to travel. The FCDO may also provide support if they need to prove their identity prior to getting a new passport.

Passport cancelled by HM Passport Office in error

If the passport has been cancelled by HM Passport Office in error, you must issue the customer with a replacement passport free of charge (gratis). This passport must be valid until the expiry date of the cancelled passport.

To issue the replacement passport, you must:

1. Send the customer an SE04 application form with a prepaid reply label.
2. Tell the customer to return the completed form with a passport photo (and any receipts) using the pre-printed label that comes with the form.
3. When the customer returns the form, issue a replacement passport:
   - in line with the LSR guidance
   - free of charge (gratis)
   - with the expiry date of the passport you are replacing (the remaining validity)
   - with a validity observation (code OBTP: replaces cancelled passport)
4. Process any out-of-pocket expenses requests from the customer.

If the customer is overseas and they need to travel urgently, you must tell the customer to contact the FCDO and request an ETD.

If a customer wants to make a complaint

If customer wants to make a complaint you must follow the complaints procedure.

Related content
Contents

How the Disclosure team deal with malicious LS reports

This section tells HM Passport Office Disclosure team staff how to deal with a customer telling us about a malicious lost and stolen (LS) report.

The Disclosure team may find out about potential malicious lost and stolen (LS) reports from the customer, if they send a ‘subject access’ request (SAR).

The Disclosure team must deal with any formal SARs or other enquiries in line with disclosures guidance.

Checking watchlist matches with Counter Fraud teams

If you find a watchlist match on an application, you must email the Counter Fraud team (CFT). In the email, you must also copy in:

- Passport Service Management team (PSMT)
- Intel Hub

In the email, you must:

- send the passport holder’s details, including:
  - full name
  - date of birth
  - place of birth
  - contact telephone number
  - contact address
  - email address
  - passport number
  - details of the malicious report
- tell CFT that you are dealing with a subject access request for information about the passport holder’s passport and loss record
- tell CFT where the request has come from

The CFT will reply and tell you if you can disclose the details on the Lost or Stolen (LS) record to the customer.

When you must not disclose to the customer

You must not disclose the loss report details to the customer, when:

- you have identified a malicious report of loss
- CFT tell you

You must send:

1. The customer a non-disclosure letter telling them the options available.
2. An email, containing the details of the malicious LSR report to Passport Service Management team (PSMT). This will then be added to the malicious report log.

Related content
Contents

How the LSR team deal with malicious LS reports

This section tells HM Passport Office Lost, Stolen and Recovered team staff how to deal with malicious reports.

The Lost, Stolen and Recovered (LSR) team deal with queries from customers about:

- lost or stolen reports (LS)
- Digital Lost or Stolen Reports (DLSR).

This contact can be:

- from the customer, by phone or email
- on a paper LS01 form
- on a digital lost and stolen report (DLSR) from gov.uk
- from staff in an Application Processing Centre (APC), for example, if the customer visits a passport office asking why their passport is recorded as lost

The LSR team will also get referrals from Sopra Steria Ltd (SSL), when they process a Digital Lost and Stolen (DLSR) report.

LSR: when the customer has not reported their passport missing

When you, the LSR team member, are contacted by a customer to tell you that they have not submitted the LS or DLSR report, you must:

1. Check the customer's details, including:
    - full name
    - date of birth
    - place of birth
    - contact telephone number
    - contact address
    - email address
    - passport number
    - details of the malicious report
2. Ask the customer to confirm they did not send us the DLSR report.
3. Check if the passport is cancelled on the Main Index (MI) database.
4. Add a LS note stating, 'customer advises that they did not cancel their passport, possible malicious report'.

Where the malicious report relates to a child passport, you must complete a watchlist check on the child's identity.

If the passport has been cancelled

If the passport has been cancelled, you must:

1. Tell the customer we will:
   - investigate
   - contact them within 10 working days
2. Send an email to PSMT with the details of the malicious report.
3. Add a LS note stating, ‘customer advises that they did not cancel their passport, possible malicious report’.

If the passport has not been cancelled

If the passport has not been cancelled, you must:

1. Tell the customer we have not cancelled the passport, but we must still report the malicious report to the police.
2. Send an email to PSMT with the details of the malicious report.
3. Add a LS note stating, ‘malicious cancellation attempt’.
4. Fail the LS record on AMS.

Related content
Contents

Passport Service Management team: malicious LS reports

This section tells HM Passport Office Passport Service Management team staff how to deal with malicious lost and stolen reports.

You, the Passport Service Management team (PSMT) staff member, will get notification of malicious reports from staff in:

- the Disclosure team
- the Lost, Stolen or Recovered (LSR) team
- Sopra Steria Ltd (SSL)
- the Customer Service Management team (CSMT)

You will get these reports by email, in to the ‘PSMT Malicious Reports’ mailbox.

Recording malicious LS reports

The PSMT Lifetime Maintenance team (LMT) must record all malicious LSR reports on the malicious report log for investigation.

This log contains all records of:

- malicious cancellations
- prevented malicious attempts

The LMT will report all lost and stolen malicious case data to the lost and stolen working group, for information purposes only.

Sending the malicious LS report for investigation

When you get a malicious LS report, you must send it for further investigation immediately.

Malicious LS reports from CSMT or an examiner

If you get a malicious LS report from CSMT or an examiner, the Intel Hub will already be aware of the report.

You must:

1. Add the customer’s details to the ‘LSR malicious complaint log’.
2. Send a copy of the details from the line on the malicious complaint log to the Security helpdesk by email.

Malicious LS reports from all other teams

When you get a referral with details of a malicious report, you must add the customer's details to the 'LSR malicious complaint log'.

Then, you must send a copy of the details from the line on the malicious complaint log by email to:

- the Security helpdesk
- Intel Hub

If the passport has been cancelled, you must also copy CSMT in to this email.

Where the malicious report is in relation to a child's passport, you must also copy Child Protection and Safeguarding team (CPST) in to this email.

Related content
Contents