CONTENTS

1. Introduction .............................................................................................................................. 3
2. When to use Electronic Identification Verification System ........................................... 3
3. Record-keeping ...................................................................................................................... 4
4. How to change password at first log-in ............................................................................ 5
5. How to log-in and select the profile .................................................................................. 7
6. Face to face verification ...................................................................................................... 8
7. Non-Face to face verification .......................................................................................... 12
8. Additional Data Entry ........................................................................................................ 15
   International Passport .................................................................................................. 16
   Electricity Supply & bill information ......................................................................... 17
   Driving Licence number ............................................................................................. 18
   Credit/Debit card number .......................................................................................... 18
   Identity Card .................................................................................................................. 19
9. Record-keeping & Compliance ......................................................................................... 20
10. FCO/MLRO Referrals ...................................................................................................... 22
1. Introduction
During Q1 2010 Intrinsic, IWM and Mint ARs and advisers begun to use electronic Identification Verification system when conducting I.D searches on their clients. Below is further information on the system and how to use it.

https://www.prove-uru.co.uk/Intrinsicfs/

**ELECTRONIC IDENTIFICATION VERIFICATION (EIDV) TRAINING** - All newly appointed advisers will have seen EIDV on the induction course. As part of your development towards Competency Adviser Status (CAS) the EIDV computer-based training must be completed and a certificate of completion provided to your Competency Development Manager before your first one to one meeting.

The EIDV training can be accessed on the relevant extranet site under Financial Crime > Electronic ID.

From 1st April 2010 all new clients and existing clients whose circumstances have changed must have their identity verified using Intrinsic’s electronic ID system EIDV. The web-based system is operated by GB Group, in partnership with BT, and is commonly used across the financial services industry as well as by large retail and gaming companies.

The profiles set up in the system exceed Joint Money Laundering Steering Group (JMLSG) guidance on electronic verification of clients. They provide you with assurance that not only are you meeting your anti-money laundering requirements to verify your client's identity but also that integrated anti-fraud monitoring tools are providing additional peace of mind that you are not becoming involved in acts of financial crime.

At times there will still be a requirement to follow a particular lenders or providers’ processes and obtain copies of client identification. This must be done in addition to the electronic ID process.

Any queries, questions or concerns about the results provided should be immediately referred to the Financial Crime Team (uru@intrinsicfs.com).

For any IT issues or password problems, please contact the Intrinsic IT Helpdesk on 01793 647499.

This is a guide to the system and provides hints and tips. The ! indicates an important piece of information for using the EIDV system.

2. When to use EIDV

EIDV is to be used only where the identity of the customer the adviser is doing business with needs to be verified. If the ID checks have been previously completed, and there is no change in the customer's information (i.e. they have not moved or changed name), then re-verification does not need to be completed. In accordance with JMLSG Guidance Part I 5.3.23:
Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification).

If the customer’s information has changed since the last time their ID was verified then their identity needs to be re-verified:

Before verifying the customer’s identity using EIDV you must have provided them with a Terms of Business containing the Financial Crime section and wording.

Further guidance can be viewed in Section 5 of the AML procedures.

3. Record-keeping

When creating a commission expectation ('contract') in OfficeWeb the adviser is required to indicate how the ID verification process has been completed and how ID records are held – ‘paper’, ‘electronic’ or ‘simplified due diligence’
Paper records may be held where ID verification has been completed prior to the adoption of the EIDV process and where those records remain appropriate. In accordance with JMLSG Guidance Part 1 5.3.23:

“Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification)”

Therefore, should further business be transacted with the client when appropriate paper records are held, the EIDV system does not need to be used, and the adviser is able to select ‘paper’ in OfficeWeb.

However, should the customer’s name or address change, or should the adviser identify through ongoing customer due diligence (fact-finding) that the relationship with the customer has materially changed or the customer poses a greater financial crime risk, their identity must be re-verified through EIDV.

Simplified due diligence should be selected when i.d verification for a client has not been carried out due to simplified due diligence conditions being met by the client (financial crime bulletin number 11). In order for simplified due diligence to be met the following should be satisfied.

- The product recommended is a General Insurance or Pure Protection contract; 
  AND
- The total premiums for all contracts being arranged are under £50 a month (£600 per Annum) or where a single premium of no more than £1800 is paid; AND
- Premiums are paid from one of the lives assureds own bank account or a joint account; AND
- There is no knowledge or suspicion that a proposed relationship or transaction involves money laundering, terrorist financing, or there are no doubts about the veracity or accuracy of documents, data or information obtained from the customer.

In the case of multiple GI & Protection policies for the same customers you must verify ID and address before application when the total premiums exceed £50 per month (e.g. Life plan for £30 and a CIC plan for £25 requires ID must be verified for all lives assured).

Equally, if the customer is not paying the contributions for the plan you must still verify their ID and address. In addition, this must be done when recommending a Whole of Life contract. However, if you are in any doubt where the ID checks should be completed, best practice would be to complete the EIDV check.

For further details on how to save EIDV results see Section 9.

⚠️ It is important that a ‘PASS’ decision is attained before an application is submitted or a Policy put "on risk". If a successful decision cannot be achieved prior to the submission of an application (e.g. a Mortgage Deal is about to end) then the Financial Crime Team should be advised of this. Failure to do any of this will result in a breach in the sales process being recorded.

4. How to change password at first log-in
1) Input the user name and password and click ‘log in’. User name will be forename.surname

2) A warning will appear “Your password must be changed…….” – then click ‘Need to change your password’:

   Account: training3@intrinsicfs.com
   Password: ********
   Need to change your password?

   Your password must be changed before you can logon

3) Input the old password, a new password (that will indicate the security strength) and re-confirm the new password. Then click ‘change password now’.
4) When the message to confirm that the password has been changed appears, click 'back'

<table>
<thead>
<tr>
<th>Change Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
</tr>
<tr>
<td>Old Password</td>
</tr>
<tr>
<td>New Password</td>
</tr>
<tr>
<td>Password Strength</td>
</tr>
<tr>
<td>Confirm Password</td>
</tr>
</tbody>
</table>

Password changed successfully

5) Finally, re-enter the new password and click 'log in'

<table>
<thead>
<tr>
<th>Log in to URU - identity verification service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please enter your account &amp; password and click log in.</td>
</tr>
<tr>
<td>Account</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

Need to change your password?

6) This will log you in to EIDV.

5. How to log-in and select the profile

You will have already been given an Account name ID and password.

Click on the following link or copy and paste the URL into your web browser:

https://www.prove-uru.co.uk/Intrinsicfs/

Save into favourites

Before doing anything else it is advised to save this webpage into your ‘Favourites’ folder in your web browser.
Log-in
Type in your Account name and password into the following area and then click

Log in to URU - identity verification service

Please enter your account & password and click log in.

Account
Password

Need to change your password?

You will be presented with this screen:

Select the profile that you require depending on how the advice has been provided to the client and click on 'continue'

6. Face to face verification

Having selected the correct profile the following information must be input in all authentications:

1) Customer data
2) Address data

It is equally important to ensure that the address details are input correctly. Therefore an address look-up facility is used.

Input the customer’s postcode and building number. Then click ‘lookup’. The available addresses will appear for selection – Click OK:
EIDV will then automatically input the correct address data into the correct fields – **DO NOT** change this format/order of information.

If the address lookup does not find the provided address automatically, select the nearest similar address and then manually change the details to the information provided by the client, keeping the same format. If the client has no street name you will need to enter a full stop in the street field in order to continue.

**DO NOT** input dates into the first and last residency year – leave these blank. You **DO NOT** need to input any previous addresses. You are trying to verify that the client lives at their current address.
Authentication
To validate and check the customer’s identity, click either of the two ‘authenticate’ buttons once:

RESULTS

- Customer Data (Forename, surname, middle initial, title, gender, DOB)
- Address Data
- Telephone Data
- 2 items from:
  Passport, Driving Licence, Electricity Supply Number and Credit/Debit card

NB: if the check results in an ALERT decision & items have been input then the authenticate button must be pressed again in order for the system to look at the item.

Refer

1) **CHECK DATA INPUT** (AND RE-INPUT IF INCORRECT)
2) IF CORRECT REFER TO FCO WITHIN 24 HRS
3) PEND RESPONSE – **DO NOT ALERT CLIENT TO RESULT**

NB: A Royal Mail redirect in the client’s name at the address input will always give a REFER decision and this must be referred to the Financial Crime Team

EIDV will automatically check online records (electoral role, credit records and landline phone records) and based on the information matched will provide one of three possible results from the *initial* authentication:

- **PASS**
- **ALERT**
- **REFER**

Each are explained further below, with details of any further action required
1) PASS
- Sufficient data has matched online records therefore no further authentication is required
- For your own records you should print/save the results as once cleared these will no longer be available
- A record of the authentication result is automatically stored in the admin system and is visible to FCO, Compliance and Supervisors for audit purposes

2) ALERT
- Insufficient data has matched and therefore further information needs to be checked to verify client’s identity
- You do not need to print/save the record
- A record of the authentication result is automatically stored in the admin system and is visible to FCO, Compliance and Supervisors for audit purposes
- You need to check (along with name/address/dob/tele info) two of the following:
  - Passport details
  - Driving Licence details (Except Northern Irish issued licence)
  - Electricity Supply & bill information
  - Credit or Debit Card details

⚠️ If this information was input initially (at Stage 4 above), then immediately click authenticate again. Otherwise the information will need to be input.
  - Having performed the re-authentication you will then obtain a PASS or REFER

FURTHER GUIDANCE ON CORRECT INPUT OF THIS ADDITIONAL INFORMATION IS CONTAINED BELOW (ADDITIONAL DATA ENTRY)
- For a PASS, for your own records you should print/save the results as once cleared these will no longer be available
- A record of the authentication result is automatically stored in the admin system and is visible to FCO, Compliance and Supervisors for audit purposes

3) REFER
- For a REFER, first check that the data entry has been correctly completed
- If it hasn’t been input correctly, amend and re-authenticate
- If it has been input correctly, or a REFER is still obtained, email The Financial Crime Team (uru@intrinsicfs.com) with the client name and date of authentication
- Further guidance or confirmation of further actions will then be provided
- During a REFER process, continue to deal with the client(s) as usual but do not alert them to the identification process.

7. Non-Face to face verification
Having selected the correct profile the following information must be input in all authentications:

1) Customer data
Input tips:
- All customer data fields are mandatory (apart from middle name)
- Middle name – if applicable, input first initial only
- Title – use the abbreviated forms e.g. Mr, Mrs, Prof, Dr
- Customer Reference – always input in the same format <Surname, Forename>

CARE – YOU NEED TO ENSURE ALL DATA INPUT INTO EIDV IS SPELT AND TRANSCRIBED CORRECTLY. ANY ERRORS WHEN INPUTTING DATA WILL RESULT IN FALSE RESULTS BEING PRODUCED.

2) Address data

It is equally important to ensure that the address details are input correctly. Therefore an address look-up facility is used.

Input the customer’s postcode and building number. Then click ‘lookup’. The available addresses will appear for selection – Click OK:

EIDV will then automatically input the correct address data into the correct fields – DO NOT change this format/order of information.

If the address lookup does not find the provided address automatically, select the nearest similar address and then manually change the details to the information provided by the client, keeping the same format. If the client has no street name you will need to enter a full stop in the street field in order to continue.
DO NOT input dates into the first and last residency year – leave these blank. You DO NOT need to input any previous addresses. You are trying to verify that the client lives at their current address.

3) Additional data
As dealing with client’s on a non-face to face basis poses additional financial crime risks two items of further data need to be input into EIDV before authenticating.

You need to obtain and input (along with name/address/dob/tele info) two of the following:
- Passport details
- Driving Licence details (Except Northern Irish issued licence)
- Electricity Supply & bill information
- Credit or Debit Card details

FURTHER GUIDANCE ON CORRECT INPUT OF THIS ADDITIONAL INFORMATION IS CONTAINED BELOW (ADDITIONAL DATA ENTRY)

Before you proceed to authentication, please double check all data entry items to be sure that they have been input correctly. Any incorrect data entry will result in the authentication failing and additional costs being incurred.

Authentication
To validate and check the customer’s identity, click either of the two ‘authenticate’ buttons:
RESULTS

EIDV will automatically check online records (electoral role, credit records and landline phone records) and then the items you have input. EIDV will then based on the information matched will provide one of three possible results from the authentication:

- PASS
- ALERT
- REFER

Each are explained further below, with details of any further action required

1) PASS
- Sufficient data has matched online records therefore no further authentication is required
- For your own records you should print/save the results as once cleared these will no longer be available
- A record of the authentication result is automatically stored in the admin system and is visible to FCO, Compliance and Supervisors for audit purposes

2) ALERT
- Insufficient data has matched and therefore further information needs to be checked to verify client’s identity. EIDV will advise you how many items are needed.
- You do not need to print/save the record
- A record of the authentication result is automatically stored in the admin system and is visible to FCO, Compliance and Supervisors for audit purposes
- You need to check (along with name/address/dob/tele info) two of the following:
  - Passport details
  - Driving Licence details (Except Northern Irish issued licence)
  - Electricity Supply & bill information
  - Credit or Debit Card details

FURTHER GUIDANCE ON CORRECT INPUT OF THIS ADDITIONAL INFORMATION IS CONTAINED BELOW (ADDITIONAL DATA ENTRY)

- For a PASS, for your own records you should print/save the results as once cleared these will no longer be available
- A record of the authentication result is automatically stored in the admin system and is visible to FCO, Compliance and Supervisors for audit purposes

3) REFER
- For a REFER, first check that the data entry has been correctly completed
- If it hasn't been input correctly, amend and re-authenticate
- If it has been input correctly, or a REFER is still obtained, email the Financial Crime Team with the client name and date of authentication
- Further guidance or confirmation of further actions will then be provided
- During a REFER process, continue to deal with the client(s) as usual but do not alert them to the identification process.

8. Additional Data Entry
For all non-face to face (remote) authentications and for face to face authentications that produce an initial ‘REFER’ result, additional data items need to be input.

You need to obtain and input (along with name/address/dob/tele info) two of the following:
- Passport details
- Driving Licence details (Except Northern Irish issued licence)
- Electricity Supply & bill information
- Credit or Debit Card details

Below is guidance on the process for completing these data items.

**Passport**

This section captures the Passport details from the consumer, with input fields:
- **Passport number**
- **Date of Expiry**

The full Passport number is entered into six consecutive fields. The Passport number is taken from the bottom line of characters on the details page of the customer’s passport.

![Passport Image]

The first field consist of 10 numbers, then 3 characters, 7 numbers, 1 character and 7 numbers. The final field is for the 2 numbers at the right-hand end of the <<<<< symbols.

For the example above, the number to be entered into EIDV would be:
1234567890 ABC1234567A1234567 12

The Date of Expiry of the Passport is also taken from this page.

**International Passport**
The same input data needs to be taken for international passport. However, as the additional chevrons (<) also need to be input. For example:

<table>
<thead>
<tr>
<th>Passport Number</th>
<th>Examples</th>
<th>Expiry Date</th>
<th>Country of Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>F3513398&lt;</td>
<td>01234567 &lt;I</td>
<td>30</td>
<td>India</td>
</tr>
<tr>
<td>5 IND 8503220</td>
<td>1 GBR 5011025</td>
<td>05 2015</td>
<td></td>
</tr>
<tr>
<td>F1505306</td>
<td>M 0810000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;</td>
<td>&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt; 2</td>
<td>2 9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M030858&lt;&lt;</td>
<td>1 GRC 999999</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F0310228</td>
<td>A123123&lt;&lt;&lt;&lt;&lt;&lt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;</td>
<td>&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;&lt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 9</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The full International Passport number entry field is split into nine sub fields. These parts can be read from the Passport in the order as follows:
- 9 characters made up of a combination of numbers and/or letters. Where less than 9 characters it will be padded out to the right with chevrons (<).
- 1 number
- 3 letters
- 7 numbers
- 1 letter
- 7 numbers
- An international passport will have up to 14 characters in this field (numbers and/or letters). If none exist, as for a British Passport, or where less than 14 characters exist, the field will be padded out, but only to the right, with chevrons (<). You should input the data exactly as it is shown on the actual passport field, i.e. input all chevrons to the left of the characters and do not ignore or leave these as blank spaces. Where less than 14 characters, the field will be padded out to the right with chevrons (<), i.e. <Z1234567<<<<<<
- 1 number or chevron
- 1 number

**Electricity Supply & bill information**

This section allows the user to check the details from a consumer’s recent (no more than 3 months old) electricity bill or statement, and comprises three fields:
- Electric Supply Number
- Mailsort number on the electricity bill
- Postcode on the electricity bill

The Electricity Supply Number has been broken into four sub fields, of length 2, 4, 4 and 3, to enable the number to be accurately obtained from the bill. On a typical bill, there will be a series of boxes printed on the bill, and may be labelled **Supply number(s)**. The boxes will appear similar to this:
The comprises five fields:

<table>
<thead>
<tr>
<th>Credit/Debit card number</th>
</tr>
</thead>
<tbody>
<tr>
<td>45 678 890</td>
</tr>
<tr>
<td>11 2222 3333 444</td>
</tr>
</tbody>
</table>

Using this example, the numbers to be entered into the Electricity Supply Number fields are 11, 2222, 3333 and 444 respectively.

The Mailsort number (if any) is printed immediately to the right of the address. The Mailsort number is a 5-digit number. Any other digits that may appear with it can be ignored.

Driving Licence number

This section captures the Driving Licence details from the customer’s driving licence photo card, with input fields:

- Driving licence number
- Date of Issue
- Postcode as stated on the driving licence

⚠️ THIS FORMAT IS ONLY VALID FOR UK ISSUED LICENCES OTHER THAN NORTHERN IRELAND AS THEY ARE NOT ISSUED BY DVLA AND HAVE A DIFFERENT LICENCE NUMBER FORMAT

The Driving Licence Number has been broken down into four sub fields. These are identified from the driving license photo card as follows:

- 5 characters (made up of letters and/or numbers)
- 6 numbers
- 3 characters (made up of letters and/or numbers)
- 2 characters

For example, a typical Driving Licence may display:

| ABCDE | 123456 | FG7HJ |

This number would then be entered into EIDV as:

ABCDE 123456 FG7 HJ

Credit/Debit card number

The Credit/Debit Card section allows the consumer's Credit/Debit Card to be proven, and comprises five fields:

- Card number
- Card expiry
- Card issue number
- Card type
- Card verification code

The Card number, Card expiry and Card type fields need to be supplied for an EIDV check.

The input data format is as follows:
- The card number should be added without spaces.
- The card expiry to be entered as 09 2011 for month/year.
- The card issue number is either one or two digits long.
- The card type will need to be selected from the drop-down list.
- The card verification code is either a 3-digit, or 4-digit (for Amex). Care is needed to identify this number as other digits may be shown before the actual code required.

Identity Card

This section captures Identity card information.

The full Identity card number entry field is split into three lines consisting of 14 fields corresponding to how they are laid out on the cards themselves.

Line 1
- 2 characters made up of letters or chevrons representing the document type (ID or PD for Germany)
- 3 characters made up of letters or chevrons representing the issuing state (D<< for Germany)
- 9 characters made up of letters or chevrons representing the document number
- 1 number representing a check digit for the document number
- 15 characters consisting of letters, numbers or chevrons

Line 2
- 6 numbers representing the date of birth of the card holder
- 1 number representing a check digit for the date of birth
- 1 character which is M, F or < representing gender
- 6 numbers representing the date of expiry of the card
- 1 number representing a check digit for the date of expiry
- 3 characters made up of letters or chevrons representing nationality
- 11 characters consisting of letters, numbers or chevrons

Line 3
- 30 characters consisting of letters, numbers or chevrons as a machine readable data
9. Record-keeping & Compliance

A record of each authentication is stored in the back-office admin system that is only accessible to certain HO and Supervisory Teams.

Therefore, you may wish to print/save a copy of the authentication for your own records. It does not need to be uploaded into the OfficeWeb sales process. Over time, full integration into the sales process will be achieved and a copy of the results will automatically be pulled back in to OfficeWeb.

Printing/saving results

Once the authentication has been completed you can print it or store an electronic copy. This is done by clicking the “printable version” icon:

![printable version]

This will open a separate window. At this point you can print this document for your paper files.

To create an electronic version select “Page” in your windows browser:
Then “Save as…."

Change the file name to “<Client name> ID” and save it as a .mht file to a location on your computer. It can then be uploaded to the OfficeWeb Document store for the relevant sales process.

Compliance and Supervision

Compliance will access the check when completing case checks and will assess the audit trail of the authentication. Records will also be viewed by your CDM or Field Supervisor as part of any T&C activity.

They will look for a final ‘Pass’ result or a ‘Fail’ with email confirmation from Financial Crime Team to proceed. The results will be recorded as part of the case check in Worksmart.
It is important that a ‘PASS’ decision is attained before an application is submitted or a Policy put “on risk”. If a successful decision cannot be achieved prior to the submission of an application (e.g.: a Mortgage Deal is about to end) then the Financial Crime Team should be advised of this. Failure to do any of this will result in a breach in the sales process being recorded.

10. Referrals

The purpose of this section is to document the advisers’ actions and subsequent Financial Crime Team actions that may be required in each of these three decisions. It also records the concession and over-ride process that the Financial Crime Team may consider appropriate.

Decision bands

The profiles that have been set EIDV system that all Intrinsic, Mint and IWM advisers are required to use to verify a client’s identity will produce one of three decision bands when the authentication process is followed.

PASS

When sufficient electronic and paper documentation checks have been completed and successfully matched the adviser is required to print and/or save a copy of the results for their own records.

ALERT

When there are insufficient electronic records to verify the customer’s identity (against electoral role, credit records and telephone records) the adviser is required to input two of four additional items of identification:

- Passport (UK or International)
- UK Driving Licence
- Electricity Supply details
- Debit/Credit Card information

Further checks are then made to verify the customers name, address and date of birth against this additional information, as well as completing checks to ensure the documentation provided is not fraudulent, by completing algorithm calculations and database checks.

Having input this documentation the result produced will be either ‘PASS’ or ‘REFER’.

In a limited number of cases the adviser may find, for valid reasons, that the client does not have two of the four additional identity documents required; and therefore will be unable to obtain a PASS decision through EIDV.

In these instances a referral must be made to the Financial Crime Team so that the EIDV check can be assessed and if applicable a concession may be granted.

REFER

A ‘REFER’ decision will be produced in the following circumstances:
1. A match against Royal Mail re-direct database
2. A match against HALO mortality database
3. Incorrect documentation data supplied or input into EIDV
4. Possibly fraudulent documentation
In the reasons 1-4 above the adviser is required to contact the Financial Crime Team for further advice and possibly a concession in order to proceed.

For reasons 5 & 6 above, the adviser will first review the area(s) of the results that has produced the ‘REFER’ decision. Should they recognise that incorrect documentation details have been supplied or input, these details should be checked and re-input.

If having reviewed the data input the adviser concludes the correct information supplied by the client or input from copy documentation has been entered into EIDV correctly the documentation may be fraudulent and adviser should contact the Financial Crime Team for further advice.

Financial Crime Team process
In the instances where a PASS decision can not be achieved due to a lack of EIDV relevant documentation or where a REFER decision occurred, the adviser should contact the Financial Crime Team immediately.

The Financial Crime Team will review the EIDV authentication and respond to the adviser within 24 hours, but usually within the same working day. The adviser will be required not to proceed with any business submission until a reply to their referral has been received UNLESS delaying any application may be of material disadvantage to the customer (e.g. tax year end or at the end of a mortgage rate).

On receipt of the referral the Financial Crime Team will assess the EIDV results and determine one of the following courses of action:

- **RE-KEY**
  Either incorrect information or inadequate information was input in to EIDV and the check needs to be re-done. The Financial Crime Team will inform the adviser of this.

- **CONCESSION**
  A concession may be granted in the circumstances where an ALERT or REFER decision can be treated as a PASS. These circumstances are below:

  **Mortality (HALO) Database - REFER**
  Initial enquiries are made back with the adviser as to why he/she might suspect a match has been made (e.g. parent with the same name).

  **Royal Mail Re-direct - REFER**
  Initial enquiries are made back with the adviser as to what he/she might think or know about why a re-direct might be set on the property. This enquiry is then considered in line with the overall EIDV check to determine the level of likelihood and if the explanation for the re-direct is reasonable in the overall context of the case, a concession will be allowed.

  **Documentation - REFER**
  If a REFER decision results from documentation checks (passport, driving licence, electricity bill or debit/credit card) further details and copies of documents will be requested.

  **Documentation - ALERT**
  In some circumstances the EIDV check will ask for more documentation however the client will not have that documentation available (e.g. expired passport, no driving licence, electricity paid by token, no debit/credit card). This is particularly relevant for elderly clients.
In these circumstances a concession can be granted if, having completed a EIDV check that has not referred for any of the reasons above, the adviser has other sufficient paper ID verification and/or a home visit recorded by an Identification Verification Certificate and concession can be allowed on the basis of part electronic and part paper identification records.

A concession will not be granted in any case where the fact-find information, EIDV check or other relevant soft-fact information indicates any doubt to the customer identity; likewise if there are any financial crime indicators present.

In all circumstances consideration will be made if the advice has been provided face to face or on a non-face to face basis.

A secondary concession and oversight process is provided through Wallace Dobbin where border-line and/or difficult cases can be discussed. There is no appeal process available following the request of a concession.

**Concession Log**
All issued concessions will be recorded under the individual adviser’s concession log in worksmart. Once the adviser has had confirmation either verbally or written that a concession has been logged in worksmart they can proceed with placing business for the client.