**From:** **Dan Tanham**

**To:** **UC Programme Board**

**Date:** **20 July 2017**

# UC Full Service identity proofing – complementary service and proofing standards

## Background

1. In 2014, Programme Board ratified that the service being offered by GOV.UK Verify (at the time called IDAP – the Identity Assurance Programme) was sufficient for UC's needs.

2. At that point in time, Cabinet Office had forecasted that GOV.UK Verify would allow 90% of UK citizens to prove their identity online. As such, the UC Programme asked the board to ratify that, contrary to an original assumption made in the business case that 'level of assurance 3' or LOA3 was required, the level of proofing provided by GOV.UK Verify known as LOA2 was sufficient.

3. Subsequently, we have seen that using GOV.UK Verify on UC achieves circa 30% success and at the UC Programme Board in January 2017, we gave an update on the development of a complementary identity proofing service ("Prove Your Identity") being built by DWP to complement the service provided by GOV.UK Verify. This service will be offered to UC claimants who are unable to successfully use GOV.UK Verify to prove their identity.

## Purpose of this paper

4. From an anti-fraud perspective, the new complementary service has a key difference in that the level of identity proofing it offers is weaker, in general identity terms, than that offered by Verify's Level of Assurance (LOA) 2 service; according to the NCSC "Good Practice Guide" definitions, the complementary service provides LOA 1 identity proofing (see Appendix for further details).

5. This paper demonstrates that this level of proofing is itself sufficient and the board is asked to accept that the mitigation measures described are sufficient to enable LOA1 ID verification.

## Why does Universal Credit need identity proofing?

6. Securing UC against criminals attempting to commit fraud, steal data and disrupt the service is a key priority for DWP. Every aspect of UC's design is explored from this perspective, assessed for risk and complemented by controls to ensure that the overall security and fraud risk of the service is within tolerance.

7. In line with best practice and in collaboration across DWP and with the National Cyber Security Centre in particular, Universal Credit has taken the approach of layering anti-fraud and security controls. Identity proofing forms part of one of these layers.

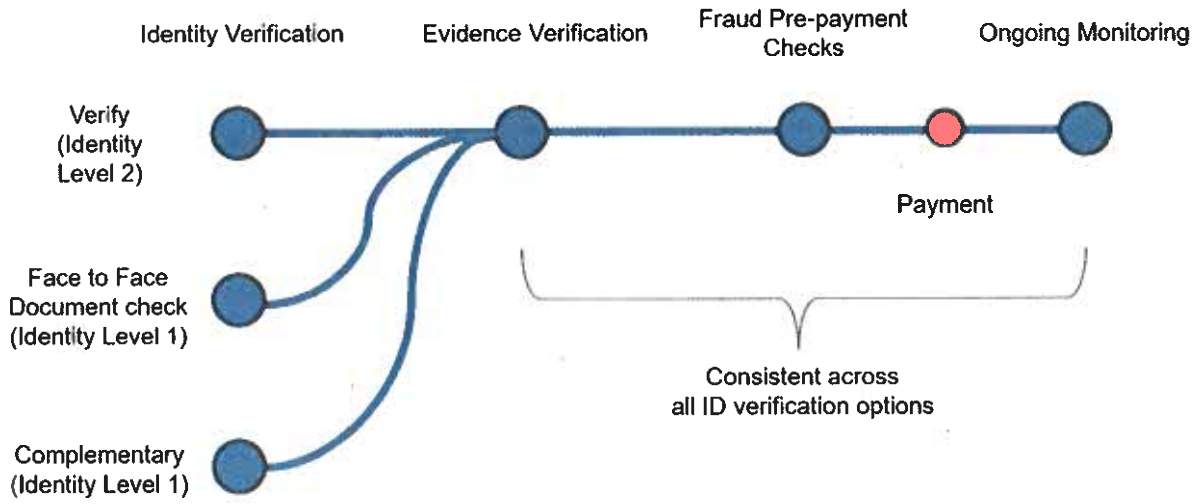


*Figure 1 – anti-fraud and security controls within UC Full Service*

8. Two categories of threat relate to identity in Universal Credit:

   a) **Impersonation or fabrication of an identity for the purpose of fraudulently claiming benefit.**

      *"James makes a claim for UC by using Mark's personal information and circumstances without his consent";*

   b) **Impersonation for the purpose of stealing personal information.**

      *"By making a claim as Mark, James attempts to access further valuable information about Mark."*

9. In this paper we show how UCFS's layers of defense, including the future use of the complementary service, provide sufficient protection.

**Recap of how the complementary service works**

10. The complementary service adds to the layers of control already in place in UC by acquiring strong proof that the claimant has access to a UK current account.

11. It does this by paying a single penny into the claimant's account, with a unique reference code. The claimant checks their statement – often on their mobile phone – and provides the unique code back to the complementary service for verification.

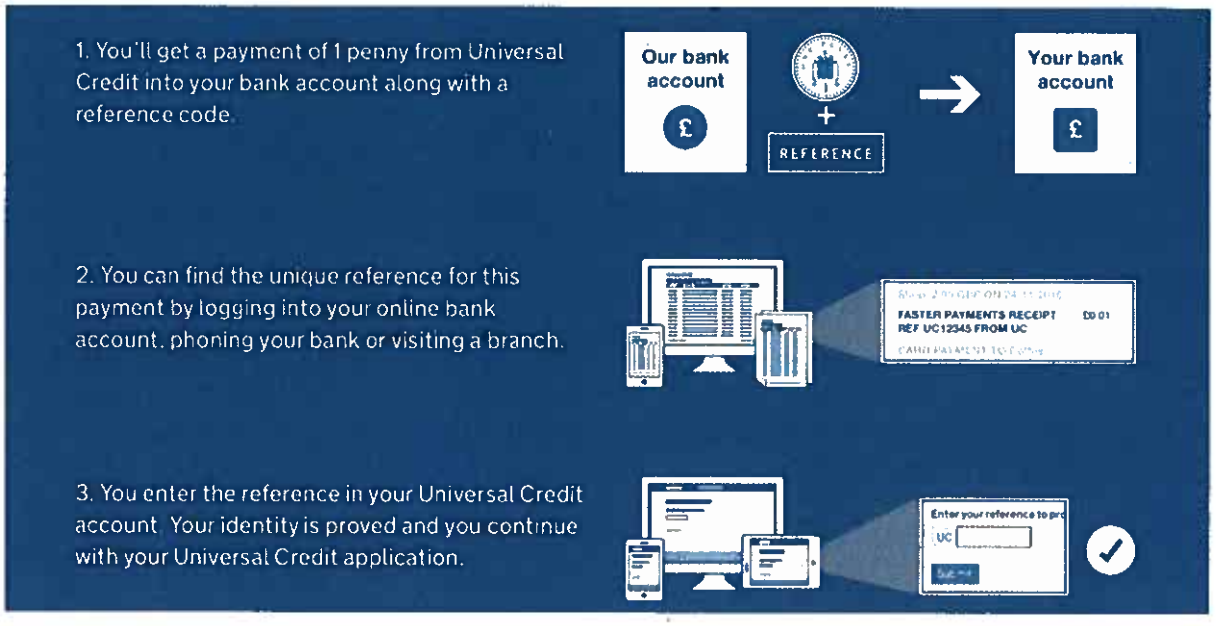


*Figure 2 - how the complementary service works*

12. The service uses authoritative reference data held by retail banks to check that the name, address and date of birth listed by the bank matches that given on the claim. In order to comply with UK anti-money laundering legislation, banks must rigorously check the identity of account holders and indeed provide ongoing monitoring of account usage.

13. This approach is currently used by third party ID proofing services and, in particular, PayPal, as a way of proving identity.

14. In terms of standards, this approach can be classed as LOA 1 identity proofing, compared with LOA 2 identity proofing offered by the current GOV.UK Verify service.

**Preventing impersonation to commit fraud**

15. The goal for this kind of attack is to fraudulently extract money from DWP. Through the complementary service we ensure that UC payments are only made to accounts matching the identity of the claimant. Therefore, in order to succeed in the fraud, an attacker would effectively need to make a claim on behalf of a legitimate claimant (who by implication would be entitled to claim UC) and subsequently compromise the claimants' banks security procedures to obtain access to the account. The fraudster would also need to provide sufficient evidence to support the other elements of the claim (for example childcare costs or housing costs).

16. Note that following an initial claim, changes to the bank account into which a claim is paid also attracts verification that the identity of the new bank account matches that of the claimant, mitigating the risk of a fraudster "taking over" a valid UC claim.

17. The DWP Cyber Resilience Centre also performs ongoing monitoring of UC accounts, which over time builds further confidence in use of the account and an ability to detect misuse or hijack by attackers.

18. Based on our analysis of this risk, supported by the Security and Resilience risk assessment team, we believe that the combination of controls offers a sufficient level of

mitigation including if identity reaches LOA 1 standard.

**Preventing theft of personal information through Universal Credit by impersonation**

19. While we believe that our set of identity controls provides sufficient mitigation of the risk of financial loss through impersonation, as cyber criminals invest in their own capabilities providing access to sensitive information over the internet is increasingly fraught. In particular, the threat posed by malicious software running on a users' device.

20. With these threats in mind, UC Full Service is designed to only display information that is strictly necessary to support the claimant in performing the task at hand. NCSC perform regular assessments of the design and have formally supported a position of its resilience to cyber fraud.

21. A design principle which has been adhered to is that no sensitive personal information is displayed back to the claimant that wasn't entered as part of the claim. Even the display of claim information is severely limited – indeed the only time that it is presented in full is at the point of legal declaration by the claimant.

22. Again, based on our analysis of this risk, supported by the Security and Resilience risk team, we believe that the controls in place (including the avoidance in many cases of this risk) are sufficient including if identify is verified to LOA 1 standard.

**Summary**

23. With the two risks above sufficiently mitigated by a range of controls as outlined, we ask that the board accept the mitigation measures as sufficient to enable LOA1 ID verification.

END

**Clearance**
Craig Eblett

**Copy List**
Mayank Prakash
Neil Couling
Ian Wright
Lara Sampson
Anthony Brigginshaw
Daniel Tanham
Claudia Natanson

## Appendix: Identity proofing level comparison

### Elements of Identity Proofing and Verification

| | A: Capture user-provided evidence | B: Validation of evidence | C: Verification | D: Counter fraud checks | E: Activity history |
|---|---|---|---|---|---|
| **LoA 2** | Collect 2 pieces of evidence that score 3-2<br><br>**or**<br><br>3 pieces that score 2-2-2 | For score-2 evidence, check it is valid **or** genuine<br><br>For score-3 evidence, check it is valid **and** genuine | Complete 1 of the following:<br><br>• knowledge based verification – static or dynamic<br>• physical verification<br>• biometric verification | Includes the following:<br><br>• mortality check<br>• identity theft check<br>• zero footprint check<br>• number of additional checks | Check 180 days of history |
| **UC FS + PYID** | Leverages banks' Know Your Customer (KYC) ID checks – multiple evidence types, LoA3 standard<br><br>Further evidence collected in support of specific claim attributes (e.g. children, earnings, health conditions) | Evidence confirmed valid and genuine during KYC processes<br><br>Bank account details and linkage to claimed identity checked via Bank Wizard Absolute | Evidence verified during KYC processes.<br><br>Control of bank account proven via:<br><br>• online banking (KBV/device/ password)<br>• Telephone banking (KBV/password/ biometrics)<br>• Printed statement (card + PIN/physical ID check) | Counter-fraud checks performed including:<br>• mortality check | History not checked, however payment not made until 1st AP has passed |