OPEN IDENTITY EXCHANGE

Using Telco Data for ID Proofing

June 2023 | Version 0.2

Produced by: Nick Mothershaw, Chief Identity Strategist

1 Introduction

This short document explores how data from mobile telcos can be used in the ID Proofing process.

Most mobile telcos offer the following services that can assist in ID proofing an individual:

- Validation of a user's name, address, date of birth and phone number against telco records. This service may include information about how long users account has been open and whether it is active, which may be used for Activity History in the context of ID Proofing
- The ability to send an SMS to the user's validated phone with a one-time code, providing 'dynamic' Knowledge Based Verification (KBV) of the user.

The use of these services, in combination with other ID proofing techniques, is explored in the context of:

- GPG45 – Identity Proofing and Validation, part of the UK Digital Identity and Attributes Trust Framework
- AML ID Proofing guidelines from the Joint Money Laundering Steering Group (JMLSG).

This document also comments on the inclusion benefits of using telco data for proofing, identifying parts of the population who may benefit because of telco services being included in ID Proofing services.

2 Leveraging Telco ID Proofing services in GPG45

The following table shows different combination of how telco proofing techniques can be used in the context of GPG45. The first set of columns shows how telco proofing techniques are used, the second show now another form of proofing technique is used in conjunction with the telco technique to achieve the profile stated.

The score achieved is listed for Evidence Strength, Evidence Validation, Activity for the telco services.

For the other technique used, the scores achieved are listed for Evidence Strength and Evidence Validation for each proofing technique.

The Verification is more complex. The verification score can come of one piece of proofing technique, or from several. When several proofing techniques are used and they are used to generate KBVs from different sources (one of the requirements of GPG45) it is the net verification score achieved that contributes to the achievement of the profile.

It is assumed that whoever the Identity Service Provider (IDSP) is who is doing the proofing will fulfil the Fraud requirement from an appropriate proofing source.

The type of user interaction is important:

- Foreground means the D Proofing Technique involves interaction with the end user.
- Background means the D Proofing Technique does not involve interaction with the end user. This is typically an API based match on the user data.

		Use of Telco					Other Proofing Technique					Net Verification Score	Fraud via IDSP	Who is this good for from an inclusion point of view?
Combination	**GPG45 Profile**	**Evidence Strength**	**Evidence Validation**	**Activity**	**Verification**	**Foreground / Background**	**Type**	**Evidence Strength**	**Evidence Validation**	**Verification**	**Foreground / Background**		**Fraud**	
Telco only	L1A	2	2 – API hit	1 - bill paid for 3 months	Medium Dynamic KBV via one time code	Foreground	N/A					1	1	Users who have no form of ID document, and no credit accounts.
Telco and Bank Account API Validation with Penny payment	M2B	2	2 – API hit	1 - bill paid for 3 months	Medium Dynamic KBV via one time code	Foreground	Bank Account	3	2 – API hit on Bank Validation Service	Medium Dynamic KBV via one time code in penny payment	Foreground	2	2	Users who do not use online banking.
Telco and Credit Account Data	M2B	2	2 – API hit	1 - bill paid for 3 months	Medium Dynamic KBV via one time code	Foreground	Credit Account	3	2 –API hit on Credit Reference Agency	2 x Dynamic Low free text KBVs (e.g., whats your last statement balance, what's your credit limit)	Foreground	2	2	Users who do not use online banking (or do not want to use it for ID purposes) but do have other credit such as mortgages, credit cards. This enables KBVs to be leveraged if the user only has one credit account.
Telco and ID Document	H2A	2	2 – API hit	1 - bill paid for 3 months		Background	3	2 – Visible Security Features are Genuine		Selfie cross check to image from document	Foreground	3		Good route to high for for users with Driving License or Passport by not able to crypto read and with no checkable bank account a d no credit accounts

The following combinations are not illustrated as they do not add value:

- Achievement of Medium via Telco data and Online Banking Logon – as Online Banking Logon achieves a M1B is its own right so telco data adds no incremental value in the context of medium.
- Any combination with Electoral Roll as this is not accepted under GPG45.

3 Leveraging Telco ID Proofing services for AML ID Proofing

The following table shows different combination of how telco proofing techniques can be used in the context of AML ID Proofing.

The first set of columns shows how telco proofing techniques are used, the second show now another form of proofing technique is used in conjunction with the telco technique to achieve the proofing combination stated.

For AML purposes it is how the combinations of proofing techniques meet JMLSG guidelines that is important. All the combinations listed here meet JMLSG guidelines.

For the other technique used, the method for evidence Validation and Verification is listed.

The Proofing Technique used for Verification is indicated.

Activity and Fraud are not considered here as Activity is not an explicit part of JMLSG guidelines and Fraud is dealt with separately and comprehensively by financial services firms.

The type of user interaction is important:

- Foreground means the D Proofing Technique involves interaction with the end user.
- Background means the D Proofing Technique does not involve interaction with the end user. This is typically an API based match on the user data.

	Use of Telco				Other Proofing Technique					Who is this good for from an inclusion point of view?
Combination	**Evidence Strength**	**Evidence Validation**	**Verification**	**Foreground / Background**	**Type**	**Evidence Strength**	**Evidence Validation**	**Verification**	**Foreground / Background**	
Telco and Bank Account	Telco	API hit		Background	Bank Account	Bank	API Hit	Online Banking Logon	Foreground	The telco account forms a second source of proof to mitigate against reliance. However, if the telco account is on a CRA then this will be more easily picked up via that route.
Telco and ID Document	Telco	API hit		Background	ID Document (with no address)	Bank	Scanned and Checked	Selfie Cross Check to image	Foreground	For AML the telco account is be the second proof / address proof to a photo ID document
Telco and ID Document	Telco	API hit	Dynamic Medium free text KBV via OTC*	Foreground	ID Document	ID Document	Scanned and Checked		Foreground	OTC to validated mobile is easier than the user having to take a selfie.
Telco and Credit Account	Telco	API hit	Dynamic Medium free text KBV via OTC*	Foreground	Credit Account	Credit Account	API hit on Credit Reference Agency		Background	OTC to validated mobile becomes the only user interaction.
Telco and Credit Account	Telco	API hit	Dynamic Medium free text KBV via OTC*	Foreground	Electoral Roll	Electoral Roll	API hit on Electoral Roll		Background	OTC to validated mobile becomes the only user interaction.

*Compliance note: For AML one time code to verified phone account forms the verification and mitigation of impersonation risk under JMLSG 5.3.89: requesting the applicant to confirm a secret code or PIN, … that links him/her incontrovertibly to the claimed electronic/digital identity – such codes, PINs, … may be supplied to a verified mobile phone,

4 Summary of Findings

From an inclusion perspective, telco proofing techniques are useful in the following circumstances:

Proofing Standard	**Areas Telcos are useful for inclusion**
GPG45	• Where users do not have an ID documents or credit accounts • Where users only have one credit account so that KBVs can be sources from the telco (one time code) and credit account (dynamic/static questions) • Where users do not use online banking. • Where users do not want to use online banking. • Are a good low friction route to a High Level of Confidence for user who do have an ID Document. Especially for those users who have no credit accounts.
AML ID Proofing	• To mitigate against reliance when a bank account is used as a proofing technique. • As a second proof to a Photo ID which has no address. • For Verification (mitigation of impersonation risk) alongside an ID document, as this is simpler than a selfie. • For Verification (mitigation of impersonation risk) alongside an credit account or electoral roll.