Identity Verification Policy

This is the Identity Verification Policy of Konec Mobile Pty Ltd ABN 34 650 761 667 and forms part of the Terms on which we provide Services. Konec Mobile reserves the right to change this Identity Verification Policy at any time and notify you by posting an updated version of the Policy on our website. The amended Policy will apply whether or not we have given you specific notice of any change. We encourage you to review this Policy periodically.

1. About the Policy

(a) Our policy for performing identity verification checks is outlined in accordance with the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017. You can refer to the full legislation at https://www.legislation.gov.au/Details/F2017L00399

(b) It is a legal requirement that any person wanting to activate a prepaid mobile phone service in their name must have their identity verified before the service can be activated. This applies to all carriage service providers in Australia.

(c) For your convenience, we process our identity verification at the point of activation, not at the point of sale of our SIM packs and plans.

(d) Your identity will be verified each time you activate an Konec Mobile SIM card.

2. Personal information you need to provide

(a) In order to activate a Konec Mobile service in your name, you will need to provide the following personal information:

a) Your full name
b) Your residential and service address for each mobile
c) A contact number and email address
d) Your date of birth, and
e) An identifying Government document number for either an Australian Driver's Licence or Medicare Card or Australian/Foreign Passport in your name.

(b) You need to provide this information each time you activate a Konec Mobile SIM card.

(c) Your personal information is subject to our privacy policy which can be viewed on our website at: https://www.konec.com.au/policies

3. How we verify your identity

We will attempt to verify your identity when activating a mobile service by the following methods.

3.1 Document Verification Service

We will check that your personal details and those on your chosen identification document match against details held in the relevant Government database using the Government's 'Document Verification Service' (DVS) which uses third party systems.

(a) This electronic method of verifying your identity is in accordance with the requirements set out in Schedule 1, Column B, item 1 of the Determination mentioned at 1.1.

(b) The identifying government document number that you provide is required to perform a once-off identity check to activate your service. The document number that you provide will not be stored in our database.

(c) By providing this information you confirm that you are authorised to provide these details to us and that you consent to us using this information to carry out an identity check verification as outlined in section 4.1.

(d) This electronic check will provide us with a result that is either a 'pass' or a 'fail'; we do not receive any other information in the response. We will be unable to tell you why a check has failed.

(e) If the result we receive is a 'pass', then your identity has been successfully identified and your SIM card activation will proceed in the usual timeframes.

(f) If the result we receive is a 'fail', this means that the information you provided could not be verified and we may choose to verify your identity using another identity verification method.

3.2 Real Time Financial Transaction

(a) We may choose to verify who you are via a Real Time Financial Transaction using a credit/debit card (but not a pre-paid card) in your name. This is in accordance with the requirements set out at schedule 1, Column B, item 4 of the Determination mentioned in 1.1 above.

(b) This method involves us confirming that you hold an account with a Financial Institution by performing a Real Time Financial transaction.

(c) If your payment for a plan upgrade during activation using a credit or debit card (but not a pre-paid card) is successful, this confirms your identity.

(d) If you save a credit or debit card (but not a prepaid card) to your account during activation, we will generate a $1 authorisation and if this is approved/confirmed, your identity is verified and your activation will progress. The authorisation will be instantly cancelled but depending on your financial institution, may take up to 7 working days to be released from your account.

4. Rejected activation requests

(a) If your SIM card activation order is rejected because we have been unable to verify your identity by the methods described in 3.1 and 3.2 above, your SIM card will remain inactive.

(b) In this case, you have 2 options;

4.b.1. You can submit a new activation order and attempt to have your identity verified electronically (which may fail again) or via a Real Time Financial Transaction.

4.b.2. You can request a refund for your SIM/Starter Pack.

(c) If you wish to request a refund of your SIM/Starter pack, you will need to satisfy the following conditions:

4.c.1. The SIM card must be inactive

4.c.2. You must call us to request a refund

4.c.3. You will need to provide the BSB and account number of a bank account so we can direct deposit your refund.

5. Change of Ownership

(a) Mobile service numbers can be transferred to a new owner upon receipt of a Change of Ownership request.

(b) The new owner must pass the ID verification requirements as if they are activating a service themselves.

(c) If the new owner is not able to have their identity verified (i.e. the result is a 'fail') we will not be able to transfer the service to them.

6. Additional Identity Verification for Porting mobile numbers

6.1 This section of the policy details the *additional* identity verification (over and above that detailed in sections 1-4) that we are required to undertake if you are porting your number to us from another provider.

6.2 The Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 was introduced to protect a customer's mobile number from theft through unauthorised porting. The standard requires the gaining provider to take additional steps to ensure that the person they are dealing with regarding the porting of a service, is the Rights of Use Holder (owner) of the number, has immediate access to a device associated with that number and authorises the port.

6.3 If you have requested to port your number to Konec Mobile, we will SMS a six digit One Time Code (OTC) to the number you wish transfer during SIM activation. You will need to enter the OTC into our website/app for verification. The activation and port can only continue if the OTC is successfully verified. This is the only method Konec Mobile uses to verify a porting service in terms of the aforementioned Industry Standard.

6.4 If the code entered into our website/app during SIM activation matches that sent to the transferring number, the activation and port request will proceed.

6.5 If you are unable to successfully verify the code for any reason, the activation and port will be cancelled and you will need to start over.

6.6 If you cannot receive the OTC because your existing SIM is faulty or the number has been cancelled or suspended, you will need to contact your existing provider to remedy this situation so that you can receive the OTC.

6.7 If the number you wish to transfer is used in a tablet or other device not capable of receiving an SMS, you will need to remove the SIM and place it in a compatible device that can receive SMS.

7. Existing customer authentication

7.1 This section of the policy details the *additional* identity verification (over and above that detailed in sections 1-4) that we are required to undertake if you are an existing customer wanting to undertake certain "high risk transactions".

7.2 The Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 was introduced to reduce the harm caused to customers when access to their personal information or telecommunications service is targeted by unauthorised persons. It requires carriage service providers to follow effective identity authentication processes to protect the security of high risk interactions.

7.3 Whenever you contact us, or we contact you via telephone, and before we provide any account or service information to you, we will ask you some security questions and send a 6 digit One Time Code to your registered email address that you will need to verify. If you do not answer the security questions correctly and or cannot verify the One Time Code, we will be unable to provide any specific account or mobile service information or support.

7.4 When you use our mobile app or website, certain requests will need to be authorised by verifying a One Time Code that we will send to your registered email address. If you cannot verify the code, the change or transaction you are requesting will not be actioned.

7.5 We have measures in place to handle situations where you genuinely cannot achieve verification by the above processes and will work with you to ensure you are not inconvenienced.

7.6 If you believe your account or service may be at risk of unauthorised access or theft, contact us so we can agree on the appropriate controls to protect your account.

7.7 If you receive a One Time Code and have not initiated any contact with us, have not been contacted by us or requested change to your account or service via app/website or telephone, contact us immediately and take actions to secure your bank and other financial accounts.