GUIDE

Customer Identity Authentication and Fraud Protection

This page sets out how VOCPhone verifies the identity of a person requesting a high-risk change to a customer account, and how to report suspected fraud.

The identity of any person requesting a high-risk change to an account is verified before the change is made. High-risk changes include porting a number, altering account details, issuing a replacement SIM, adding or removing an authorised representative, and disclosing account information. Verification uses more than one factor. A notification is sent whenever a high-risk request is initiated, and no charge applies to those messages.

The short version

Outcome under the Determination	Examples
Loss of access to the telecommunications service	Porting a number to another provider; transferring, suspending or cancelling a service; issuing a replacement SIM.
A change to information held about the customer	Altering personal information, business information, or account security information such as a password, PIN or recorded contact details.
Addition or removal of an authorised representative	Granting another person the ability to act on the account, or withdrawing that ability.
Disclosure of information to the requesting person	Reading out or sending personal information, business information or account security information held on the account.

Also worth knowing

Principle	Application
More than one factor	Depending on the contact method and the nature of the request, verification may combine information already held on the account, a one-time PIN sent to a trusted contact number.
A single detail is not sufficient	Knowledge of an address or date of birth does not authenticate a person. Information of that kind is routinely exposed in data breaches at other organisations.
Notification is sent	When a high-risk interaction is initiated on an account, a notification is sent advising what has been requested and what to do if it was not authorised.
No charge applies	No fee is charged for messages or notifications relating to identity authentication or to the initiation of a high-risk customer interaction, as required by section 15.
Verification is a precondition	Where the process cannot be completed, the request does not proceed.
Records are retained	High-risk customer interactions are recorded, as required by the Determination, providing an auditable record if a transaction is subsequently disputed.

1. Identity authentication before high-risk transactions

To protect customers from unauthorised high-risk customer interactions, **VOCPhone will use identity authentication processes to authenticate the identity of the person making a request, prior to undertaking a high-risk customer transaction.** This applies to all customers on every occasion.

Questions the full guide answers

- [ ] Why must my identity be verified before changes are made to my account?
- [ ] What is a high-risk customer transaction?
- [ ] I have a virtual mobile number rather than a SIM. Do these protections apply?
- [ ] How is identity verified?
- [ ] Will I ever be asked to read out a PIN or code?
- [ ] What happens if I cannot complete a standard identity check?
- [ ] I received a notification about a change I did not request. What should I do?

This is the summary. The guide has the detail.

Every point above is worked through in full on our site, with the Australian context, the numbers and the exceptions. If you would rather talk it through, call **1300 663 222** or visit **vocphone.com/about/contact-us.**