Article title

Mobility Postpaid Account Authentication and Access Policy

Article summary

This article explains the Mobility Account Authentication and Access policy and processes involved in authenticating wireless customer accounts.

Article detail

The Mobility Account Authentication & Access Policy ensures agents provide the correct access level to each caller, based on verification and account type.

- AT&T Wireless Postpaid Consumer Account Access Policy ensures customer service representatives provide the correct access level to each caller based on authentication and account type.
- Refer to the **Account Access Permissions Matrix** (which is based upon the caller's authentication and account type).

  Heads up! This list is not all inclusive.

- Looking for prepaid account authentication? See the **AT&T PREPAID Account Access Policy**.

Not what you're looking for? Check out these articles formerly included in the Wireless Postpaid Consumer Account Authentication and Access Policy (myCSP).

Article description	Article
BAN specific guidelines for authenticating the wireless account holder	**Authenticate Wireless Account Holder**

When the caller is not the account holder	**Authenticate Wireless User or Calling on Behalf of Account Holder**
Call types such as attorney's, law enforcement, prepaid, etc.	**Wireless Authentication - Special Call Type Instructions**

Heads up!

- A valid business reason is required to access customer accounts.
- Before accessing the customer's account in any interaction, you must properly authenticate the customer.
- Always document every customer interaction and use the correct disposition reason code.
- For international plans and features, only the account holder can add to, remove, or make changes to an account.

What I need to know

For all inbound calls, authentication is required at the beginning of the customer contact. Existing customer accounts need to be authenticated prior to any discussion or comment about the account.

- Agents should authenticate inbound calls from AT&T employees, vendors, and agents requesting customer information and use the same authentication process and customer credentials that a customer uses.
- There are no exceptions to the existing customer account authentication requirements for employees, vendors, and agents.
- Approval from the account holder may be required before performing a credit check.

Passcodes

1. Establish a Personalized Passcode on every account.
2. The Personalized Passcode can only be established or changed by the account holder.
    a. Explain to the customer that establishing passcodes is a standard security measure.
    b. Unauthenticated customers cannot opt out or delete a passcode that is on their account.
    c. Non-account holders are not permitted to make changes to or add a passcode to an account.
3. Follow instructions in the **Telegence Account Information Changes - Account (Security) Passcode** to establish or change the Personalized Passcode.
4. Remember: Only the account holder can add to or make changes to an account passcode!

Start the customer interaction

1. Greet the caller and introduce yourself.
2. Verify the customer account number (CTN) for the account they are calling about.
3. Ask who you are speaking with.
    a. If the caller's name matches the account name, the caller should be the account holder.
    b. If the caller's name does not match the account name, ask the caller to give you the first and last name of the account holder on the account they want to talk about.
4. The caller needs to verify the first and last name of the account holder to proceed to the next step - authentication.

Authentication

When Using Clarify

1. If Clarify shows *Passcode - IVR Verified* and you confirm the number presented is the one the customer is referencing, follow procedures in the **Account Access Permissions Matrix** for authenticated callers.

a. If changing the number, Verify that the CTN to be discussed is on the same billing account number (BAN) as the number presented.

2. If:
   a. Clarify does not show Passcode – IVR Verified or Verified Successfully, or
   b. The number represented is not the one the caller is referring to, or
   c. There is no number populated in Clarify

   Manually authenticate the customer. Reference: **Authenticate Wireless Account Holder**.

3. Within the application, Select the appropriate caller type for options to appear correctly.
4. Dual SIM: Authenticate each BAN separately based on policies for the BAN type. For more information, see **Dual SIM / Dual Standby (DSDS)**.

Manual Authentication

- Manually authenticate accounts in systems that are not equipped with a Passcode – IVR Verified or Verified Successfully flag indicator.
- Only the account holder can add to or make changes to an account passcode.
- **Authenticate Wireless Account Holder** provides BAN specific guidelines for authenticating the wireless account holder.
- **Authenticate Wireless User or Calling on Behalf of Account Holder** covers the process for authentication which is required at the beginning of the customer contact on all inbound calls.