
Member Services Verification Procedures-(updated: 10/3/24)

Adherence to the following member verification procedures is required to positively identify each member over the phone. Failure to follow proper Verification steps (security protocols) will result in Administrative Action being taken, which can include termination of employment.

The goal of verification is to protect our members and to keep their accounts safe and secure. It is important to ask verification questions that cannot be found on a statement, which can be stolen from a mailbox, or information found in a wallet that has been stolen. When verifying a Caller, ask strong “out of wallet” questions (approved questions are provided below).

The more vague or incorrect the Caller’s answers are, the more security measures need to be applied. Contact a Member Services Support Team Member or ERM-Security immediately should you suspect fraud on a member’s account.

Guiding Points and Requirements

- If **Verbal Password** is present it must be correctly provided by the Caller, no exceptions. MSRs cannot confirm to a Caller that a spoken password is incorrect. MSRs cannot provide password “hints” to a Caller. The Caller can, however, be asked to repeat the given password for clarity.
- A small percentage of members have a note to “ID Password Only”. For such members, only the member’s name, account number and password will be used during verification. Under no circumstance can a Call Center employee add a Password Only note to a DNA profile. All requests to do so must be escalated to a Director-level Support Team member. Even for these members **Full Verification**, in addition to providing the correct password, may be needed for certain requests ([see Page 3](#)).
- Read all notes and take appropriate action in assisting members. The notes are listed on the Relationship Profile by clicking “More” and “All Notes”. You must go to the notes tab for each member after you pull up the account.
- **If you spoke with a member, that was successfully verified within the same business day, you may conduct a callback to that member without going through additional verification. The call must be placed to a phone number currently on the member’s DNA profile, and you must verbally confirm that you are conducting a callback on a recorded line.**
- Recent contact information changes (examples: address, email and phone number) can indicate a potential Yellow flag situation. When there has been a change of address, email or phone number within the last 30 days extra caution should be taken.

These types of changes are listed on the Relationship Profile: Click “More” and “Address Change Inquiry”.

- All owners, Primary and Joint, will have their own Relationship Profile in DNA. Ensure that the profile for the person that you are speaking with is being used during the verification process.
- If a **Fully Verified** (see steps on Page 4) member wants to give permission for an MSR to speak to a non-owner about their account/loan they must be advised that the permission is for the current call only. If the member wants the non-owner to receive ongoing information on the account/loan that person must be added to the account/loan. The MSR must seek clarification from the **Fully Verified** account Owner on what information can be shared with the non-owner.
- Warm transfers from 3rd parties (examples: PSCU & FISERV) require verification on a line where you are sure the 3rd party is not listening in. You must call the member back on a newly established secure line.
- If the call is coming from the Georgia Relay Service for the Deaf, contact a member of the Support Team to handle the call.
- Read and take appropriate action on any Restrictions that pop-up on the member profile. At no time should an employee remove a Restriction for a Resolution or Bank On account holder.
- If an active call disconnects MSRs must attempt to reestablish contact. If the MSR is unable to reestablish contact they must add DNA notes that they attempted to do so (set note expiration for 3 days). **If abusive, explicit, belittling or degrading language was used by a Caller prior to disconnecting the line MSRs are not encouraged to reestablish contact. In cases like this MSRs must add DNA notes detailing the interaction (2-year expiration), and notify Member Services Support and report the inappropriate behavior.**
- When an incoming call is answered, but no one speaks, MSRs must provide 3 attempts for the Caller to respond before ending the call. MSRs must use the following phrase 3 times before ending the call: ***“Caller I am unable to hear you. If you are there please be sure that your line is not muted”***. Wait 3 seconds for a response and repeat the phrase. After all attempts are exhausted state the following: ***“Caller I am sorry that I was unable to assist you. If you still need help please call us back at (404) 874-1166. Thank you”***.
- If the purpose of the call involves the mailing of documents, debit cards, credit cards, checks, statements, etc. you must confirm the current full address before mailing anything out.
- If the incoming call status in Smart Suite is: **AUTHENTICATED** the Caller was successful in pre-verifying the Member # or SSN, the Date of Birth, and Zip Code.
- If the status in Smart Suite is: **NOT AUTHENTICATED** or **VERIFIED** the Caller was not successful in pre-verifying the Member # or SSN, the Date of Birth, and Zip Code.

Granting Access to Services- If the caller is requesting any of the following, **Full Verification** is required.

- Giving permission for an MSR to speak with a person that is not on their account/loan
- Closing a Savings account or Membership
- One Time Passcode (OTP) for Payrailz
- Ordering Debit/Credit Card
- Ordering Checks
- Add travel and merchant exceptions
- Adding/Removing a Password
- Address / Phone Number / Email Change
- Online Banking Unlock – Temporary OLB Password
- Providing/Confirming Account Number
- Providing/Confirming Member Number
- Tele-talk Reset
- Clearing a Fraud Alert-unblock/unlock debit or credit card
- Reactivation of disabled OLB profiles

Smart Suite

AUTHENTICATED Calls

1. Verify Name of caller matches account holder's name.
2. **Verify Verbal Password (if applicable).**
3. Ask 1 approved Out of Wallet Question. If caller is unable to correctly answer Out of Wallet Question, use Quiq to send **eligible** members an SMS text message; sent to the cell phone number on file. SMS text cannot be used if cellphone number was changed within the last 30 days. Check Address Change Inquiry in DNA.
 - **Important:** If caller is not eligible for SMS text via Quiq, or is unwilling to receive text messaging, they cannot be assisted by an MSR. They must either visit a local branch for assistance. Or, the call must be escalated to the Support Team.

NOT AUTHENTICATED or VERIFIED Calls

1. Verify Member Number OR Account Number. If caller does not have either you may use the Full SSN. Only use one option.
2. *Verify Name*, Date of Birth and FULL address on Account.
3. Verify Last 4 of SSN, if not used in step 1
4. Ask 1 approved Out of Wallet Question
5. **Verify the Verbal Password (if applicable)** -If no Verbal Password is listed use Quiq to send **eligible** members an SMS text message; sent to the cell phone number on file. SMS text cannot be used if cellphone number was changed within the last 30 days. Check Address Change Inquiry in DNA.
 - **Important:** If caller is not eligible for SMS text via Quiq, or is unwilling to receive text messaging, a second Out of Wallet question must be correctly answered. If caller cannot answer the second Out of Wallet question, they must either visit a local branch for assistance. Or, the call must be escalated to the Support Team.

If the call status does not display in Smart Suite utilize the **Full Verification** steps below.

1. Verify Member Number, Account Number OR Full SSN – Only pick one
2. Verify Name, Date of Birth and FULL address on Account
3. Verify Last 4 of SSN, if not used in step 1
4. **Verify the Password (if applicable)**
5. Ask 2 Out of Wallet Questions
6. If the caller is unable to answer the second required Out of Wallet Question, **eligible** Callers may receive a Verification SMS text message sent to the cellphone number on file. SMS text cannot be used if cellphone number was changed within the last 30 days. Check Address Change Inquiry in DNA.
7. If caller is not eligible for SMS text they must either visit a local branch for assistance. Or, the call must be escalated to the Support Team.

*****Do not use recent Deposits, Withdrawals, or other Account transactions as an Out of Wallet Question. The Smart Help feature gives this type of information to callers before reaching MSRs.*****

Out of Wallet Questions:

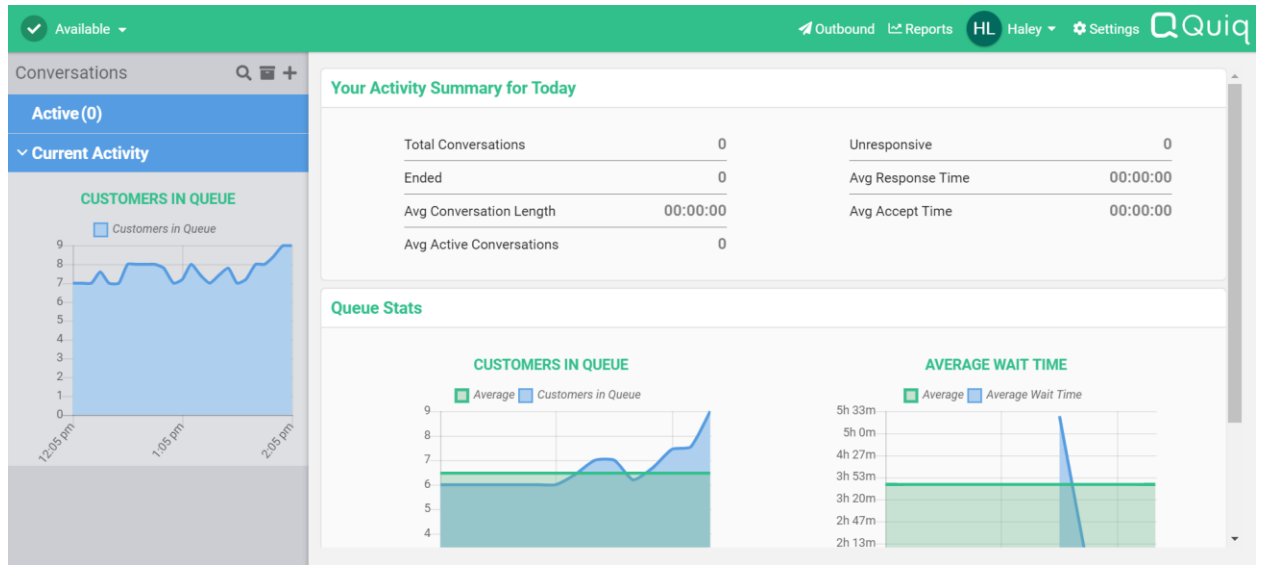
1. What is the email address that we have on file for you? ***Be sure to check if the email address has been changed in the last 30 days. If it has, do not use this question.**
2. In what year did you open your membership at Georgia's Own?
3. What is the name of the current employer that we have on file for you? If retired-What company/profession did you retire from?
4. How did you qualify for membership (**employer, family member, community, etc.**)?
5. Who was your employer when you opened your Primary Savings account?
6. Do you have a credit card with us? > If they do, ask them what the limit is. ***This is a two-part question.**
7. Do you have an auto loan with us? If they do, ask them for the Year, Make, Model? ***This is a two-part question.**
8. What was your previous address?
9. What date did you open your loan (**non-LOCs**)? Or, what is the term on your car loan? **Be specific** if the member has multiple loans. Which loan are you asking the caller about? **You could also ask the caller what are the kinds of loans they have with us if there are multiple loans.**
10. Employment Service date
11. Who are the PODs or beneficiaries on your account (**be specific about which account you are asking about**)?
12. What was your employer's address when you opened your membership with Georgia's Own?
13. What was your home address when you opened your membership with Georgia's Own (**if different than current address**)?
14. What was your job title at the time you opened your membership?
15. What is the date of formation for your business account (**if applicable**)? Located on the Secretary of State document.
16. What is the EIN for your business account (**if applicable**)?
17. What is the date of incorporation of your business account (**if applicable**)?

Quiq Navigation

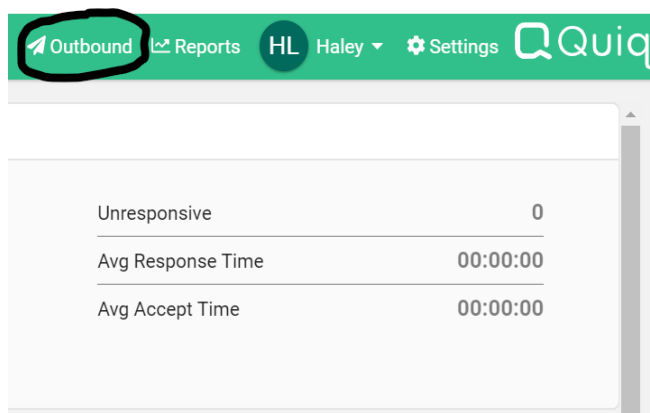
Before offering the SMS Verification code option, please complete the following checklist items.

- Confirm that Caller is willing to receive a text via SMS.
- Ensure the phone number on file has not been changed in the last 30 days
- Confirm the phone number you are messaging can receive SMS Messages.

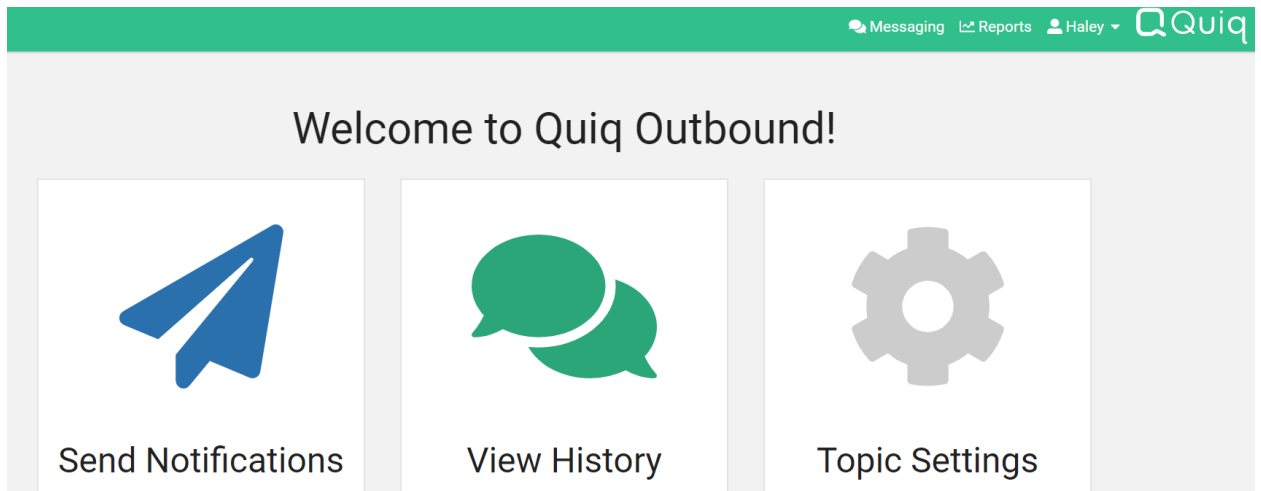
1. Login to Quiq (<https://quiq.com/>)



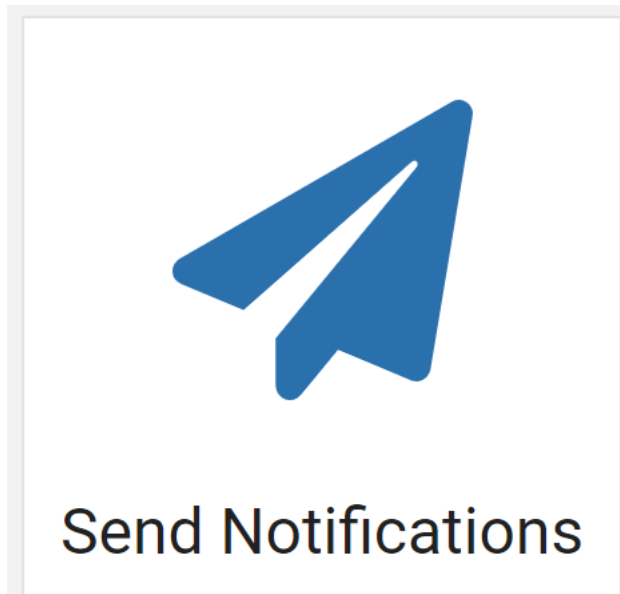
2. Select the “Outbound” icon in the top green bar



3. You will be redirected to the Outbound message portal



4. Select "Send Notifications"




5. You will now see the Outbound Notification screen

Outbound / Send Notifications


Send Outbound Notifications



Send from
(None) ▼

Topic
default ▼ 

Message Form CSV

Outbound Numbers (comma separated) *

 Show Preview

 Message 

6. On the “Send from” drop down select **Main**

Send from
Main

7. On the “Send from” drop down select **Verification Code**

Topic
Verification Code

8. In the “Message Form” Section input the member’s phone number on file

Message Form CSV

Outbound Numbers (comma separated) *

Input Member Phone Number Here

9. Read the following disclosure out loud to the member:
 - a. **“Please be advised, message and data rates may apply. At no time should you reply to the one-time code message that you receive. No response inbox has been established. And your inquiry will not receive an answer.”**
10. After the member agrees, Input the following in the “Message Form” Section by selecting the Snippet:

- a. After clicking Snippet, it will state: “Your one-time Georgia’s Own Credit Union Verification Code is: XXXXX”
 - i. *Please note, everyone has their own unique code. Do not send out any codes that have not been assigned to you.

11. Once the member receives the message they will verbally repeat the code to you and you can proceed with assisting them.

***Please note, once the message has been sent the screen will not refresh. As a result, all you will need to do the next time you send a code, is input the new phone number.**