HTS Account Access - FREQUENTLY ASKED QUESTIONS

This document provides a comprehensive list of common FAQs for High Touch Support (HTS), with a special focus on questions frequently asked during onboarding. It covers commonly asked questions related to the AA (Account Access) workflow, aiming to help new team members understand key processes, challenges, and protocols involved in supporting the workflow effectively.

Q) Can we work on accounts where the user says they are attempting to regain access to a business account?
A (Yes - you can treat these accounts the same as the regular user accounts)

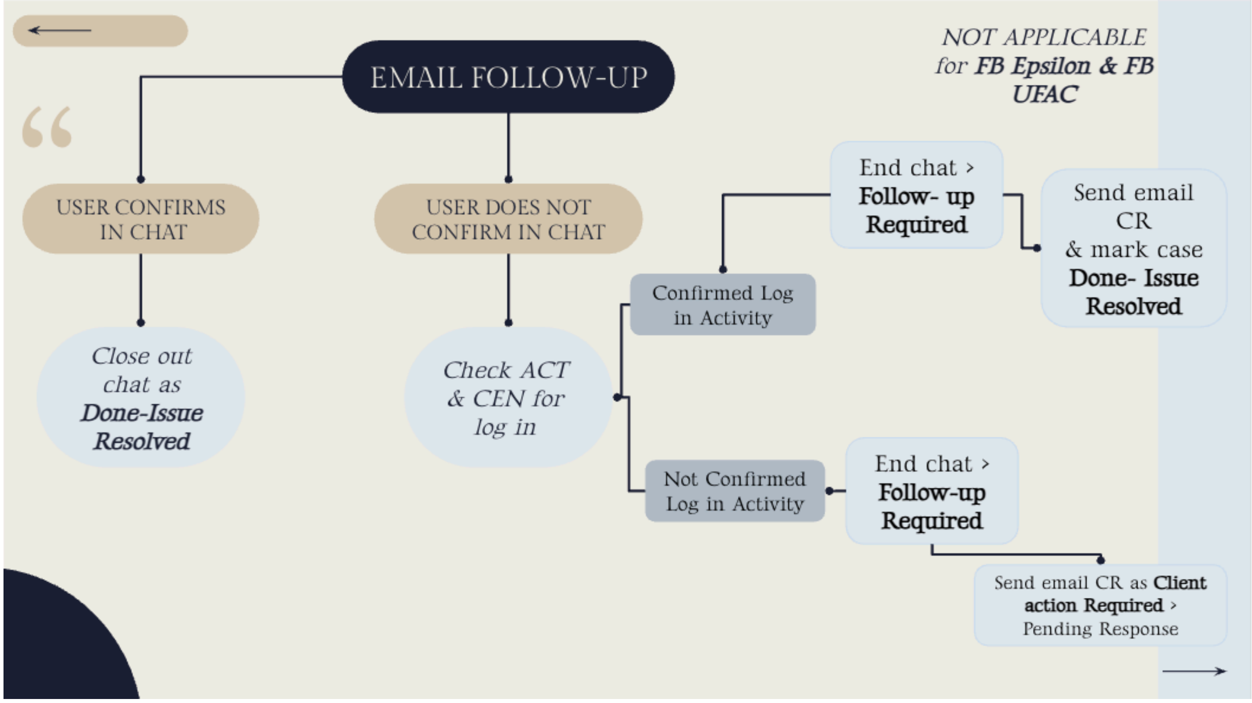
Q)How would we close a case where we solve the user's issue, but the user has another question that is out of scope or something we can't assist with? Would we close the case based on the new issue, or would we close the case for the original issue the user came in for?
A (You would close the case based on the original question the user asked.)

Q: Is the Comp Classifier output 100% accurate?
A: There will be some exceptions where manual investigation will be required - please refer to the table below (Source Launch and Rollout Plan for Compromise Classifier in HTS Workflow)

User Confirmed Issue	Comp Classifier	Next Step
Hacked or Hacked Disabled	Compromised	Proceed with Authentication (you can skip investigation step 3 & 4 below)
Hacked or Hacked Disabled	Not Compromised	Continue to investigate the account to identify the exact issue and follow the BAU manual investigation process
Account Locked, Two Fac Issues, Password Reset, Update Contact point	Not Compromised	Proceed with Authentication
Account Locked, Two Fac Issues, Password Reset, Update Contact point	Compromised	Continue to investigate the account to identify the exact issue and follow the BAU manual investigation process

Q: What happens when a user's selfie video does not match the account photos at all?
A: Close the case as **Done - Support Abuse** since they are a bad actor

Q: When would I send a follow-up email to the user?
A:



NOT APPLICABLE for ***FB Epsilon & FB UFAC***

EMAIL FOLLOW-UP

USER CONFIRMS IN CHAT

Close out chat as ***Done-Issue Resolved***

USER DOES NOT CONFIRM IN CHAT

Check ACT & CEN for log in

Confirmed Log in Activity

End chat › **Follow- up Required**

Send email CR & mark case **Done- Issue Resolved**

Not Confirmed Log in Activity

End chat › **Follow-up Required**

Send email CR as **Client action Required** › Pending Response

A: Email Follow-Up Process

1. Determine User Confirmation in Chat

1. Check if the user confirms resolution in chat:
    - If Yes:
        - Close out chat as "Done – Issue Resolved."
    - If No:
        - Proceed to check ACT & CEN for login activity.

2. Check ACT & CEN for Login Activity

2. Review ACT & CEN systems for user login:
    - If Login Activity is Confirmed:

    1. End chat and mark as "Follow-up Required."
    2. Send follow-up email with case resolution (CR).
    3. Mark case as "Done – Issue Resolved."
- If Login Activity is Not Confirmed:
    1. End chat and mark as "Follow-up Required."
    2. Send follow-up email with case resolution (CR), indicating "Client Action Required."
    3. Mark case as "Pending Response."

Q: What do I do if the user keeps emailing back and reopening their case with questions we are not able to support?
A:

- Scenario 1: If the users account was originally secured/resolved, we would continue to tell the user we are unable to assist with their new request and close the case as “Done - Issue Resolved”. After so many times telling the user we are unable to assist with their request you should get with your Team Lead who might direct you to close the case as “Support Abuse”.
- Scenario 2: If the user was denied closure or recovery but keeps reopening their case (via email). You would continue to tell the user that we are unable to assist with their request and close the case with whatever case status you originally closed it as. After so many times telling the user we are unable to assist with their request you should get with your Team Lead who might direct you to close the case as “Support Abuse”.

Q: When the user does not have images on the account, how do I authenticate them?
A: You can leverage the Contact Point Verificaiton challenge and the KBA challenge.

Q: How many points are needed to pass the authentication process for a hacked user?
A: 1 authenticity point, and 2 ownership points for high-risk entry points; 1 ownership point for mid-risk entry points but selfie is a mandatory step in this case.

Q: Can you send the selfie instructions to any email address the user provides to you?
A: Yes that is allowed.

Q: How long does a user have to submit the video once we have converted to email?
A: The user must respond with their selfie video within two days.