HTS UFAC – 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 UFAC (Unified Fake Account Checkpoint) workflow, aiming to help new team members understand key processes, challenges, and protocols involved in supporting the workflow effectively.

Q)How long can a video be sent for authviz and still be used for the Authenticity step prior to the agent having engagement with the user?
A)>4hours

Q: If a user claims they are hacked, and you confirm the activity on the account is of hacked nature, what is the issue type of the case?
A: Hacked and disabled asset

Q: If a user already submitted a selfie video before the case began, do I ask for a new selfie?
A: If the selfie was submitted within 4 hours of the case creation, then you do **not** need to ask for a new selfie.

Q: Do we have to verify contact points in the UFAC recovery process?
A: No, we do not have to verify a user's contact point in the UFAC recovery process because the user is already logged in to their account.

Q: How long does a user have to Appeal their account?
A: A user has 180 days to appeal their account before it is permanently deleted.

Q: Is a user's account visible on facebook while in a disabled status?
A: No, the user's account is not visible on facebook until they have appealed and the account has been reactivated.

Q: If a user states they are hacked do we transfer the case to Account Access?
A:

For Austin-based team: No, you will work the case as compromised, by investigating the account and proceeding with the recovery steps listed in protocol. If not hacked, treat it as a normal UFAC case.

For Dublin, FT & San Antonio teams: No, you will assign the playbook tag as Hacked and Disabled asset, but work the case same as regular UFAC case. Please advise the user to complete a security checkup upon regaining access to their account, including updating their passwords and linked emails, removing any unknown or unauthorized logins, phone numbers and emails, and reviewing all recent activity.