SecureShop®

CALL CENTER GUIDELINES

When apps offer one-to-one interactions in order to activate, get support for, return, upgrade, oftentimes they utilize a call center model. The basic idea is that call centers not only will provide the first-tier support to the consumer, but they will also make offers for other products and services. Many call centers provide this first-tier support for free to apps, and in return pay commissions to the app vendor whenever sales are made to the consumer.

This business model has led to fraudulent behavior in the software monetization industry. We want to be sure consumers aren't exposed to bad call center behavior while they use certified apps, so we have a requirement that certified apps must self-certify their internal call center operations against these Call Center Requirements. We also have additional requirements for apps utilizing call centers: (apps must have prominent non-interactive ways to get support) and (apps must disclose when additional products and services may be offered).

We built these Call Center requirements by consulting with representatives from the call center industry and attempting to implement the intent behind the FTC's' guidelines. We have reviewed them with our compliance partners, security parthers, and consumer rights groups.

Some of the requirements are marked in red and preceded by two asterisks. We consider a call center that violates these red requirements during their app interactions as a Deceptor. If we find a Deceptor, we will recommend that our partners block access to these call centers. While we want call centers to meet all of our requirements, we have set a minimum bar so our partners can protect consumers more effectively.

This glossary will help as you read through these requirements.App vendor: the owner of the app who contracts the call center to provide app interactions on their behalf.
App interaction: this is a consumer getting 1:1 interaction with the call center in order to get something done in the app. This may include getting an activation code, getting support, asking for a return. These are sourced from the app's user experience as well as the app's websites.

App activation: a common reason that consumers interact with call centers: obtaining a license key to unlock app features.

Agent: the employee or subcontractor or partner who handles the app interaction on behalf of the call center.

App workflows: the script the agent uses during an app interaction.

Diagnostics: when the agent uses remote tools and other software to diagnose the consumer's issue.

Remote access session: when the agent connects to the consumer's machine to diagnose issues during the app interaction.

Offer: once the reason for the interaction is satisfied, and maybe after diagnostics, the agent may offer additional products or services.

Conversion: when the consumer chooses to accept the offer.

Existing Business Relationship: Once a consumer has converted, they are deemed to have an existing business relationship with the call center.

Non-app interaction: when a consumer interacts with the service (not the app), post-conversion.

App interaction scorecard: how interactions are measured by the call center QA team as to whether the interaction met at least these call center requirements and the app's approved app workflows.

Cold outbound interaction: when call centers reach out to consumers to whom they don't have an existing business relationship.

OPERATIONS

(CCR-001) Call center must not mix app interactions with other businesses.
Call center agents supporting app interactions must be dedicated to app interactions. No pop-up ad-driven calls are allowed. Agent KPIs and rewards should be solely focused on app interactions. No mixing app interactions with other businesses.

(CCR-002) At least 5% of non-converted app interactions must be monitored for quality, reviewed for fraud, and scored against an app interaction scorecard within 48 hours of the interaction. The monitoring must ensure every agent has had at least 5% of their non-converted calls reviewed each quarter.
The intent is to ensure that even the most trusted agents must have monitoring of their app interactions.

(CCR-003) Every app interaction resulting in a conversion, and every app interaction regarding a return must be reviewed for fraud and scored against an app interaction scorecard.
Scoring is an important way of measuring if the consumer was adequately informed, was not unpleasantly surprised, and does not feel cheated. It also helps detect fraud committed by the consumer and by the call center.

(CCR-004) All app interactions and remote access sessions must be recorded and available for review/audit upon request by app vendor and AppEsteem for no less than 90 days. Reasonable attempts must be made to link the interaction and remote access session data to the app. Reasonable attempts must be made to remove any PII before AppEsteem reviews/audits.

The intent is that both the interaction as well as the remote session can be viewed internally, as well as by those auditing. Linking the interaction may be done many ways, for example interaction id, consumer name, phone number, license key, email address. When following up with an email to a consumer, provide a unique interaction id that can be used in the future to retrieve the interaction.

(CCR-005) Have a continuous fraud monitoring system that looks to detect and eliminate fraud caused by agents, app vendors, and service providers.
A robust fraud prevention plan is essential to ensuring consumers are never taken advantage of.

(CCR-007) App interaction scorecards must include scores for complying to at least these call center requirements and approved app workflows. Scores must matter to the continued engagement or employment of agents.
The intent is to continually measure and catch issues as quickly as possible.

(CCR-008) Have an ongoing process for identifying and returning duplicate app activations as well as conversions.
The intent is to ensure a consumer doesn't end up pay twice for activations, or for call center-offered products and services.

(CCR-009) Have an ongoing process for monitoring and responding to online reputation systems.
Tracking and responding to poor reputation is a good demonstration that the call center cares about how it treats consumers, and works to improve bad experiences.

(CCR-011) For the previous twelve months, call center has held all applicable licenses, followed the regulations for the jurisdiction in which it resides, and operated as a viable call center.
Various country and local laws and regulations govern the use of telecom, training, and business licenses.

(CCR-012) Call center must have an ongoing compliance program that includes quarterly reviews of call center compliance with FTC guidelines, these call center requirements, and country/local laws and regulations.
Call centers must perform their own internal compliance review processes. This requirement is about the compliance of the call center; not the compliance of the app or app vendor.

ONBOARDING

(CCR-013) Call center must have its own procedures to not allow app interactions for Deceptor apps. Call center must require all apps to either be certified or reviewed by AppEsteem and determined not a Deceptor.
Deceptive and fraudulent apps should not be able claim they are using certified call centers.

(CCR-015) App workflows must not have outcomes where issues can only be solved with additional offers, no matter the diagnosis. App workflows must have clear scenarios as to when products and services may be offered, and when they must not be offered.
The job first and foremost is to handle the reason the consumer needed the app interaction, and not to only to offer additional products and services.

APP INTERACTIONS

**(CCR-017) Call centers must never use deceptive, misleading, threatening, aggressive, or unethical practices during app interactions. If the consumer seems under pressure or confused, call center may not offer additional products or services.
The consumer must never feel pressured for a decision on an offer, and never allowed to accept an offer when they demonstrate they are under pressure or confused. Examples of this include scare tactics, high pressure sales techniques, false senses of urgency, non-publicly available time-bound offers, inaccurate or misleading representation, harassment or intimidation, inflammatory or designed to install unwarranted fear or concern. It also means that when consumers seem under pressure, the agent/employee is to refrain from making offers.

**(CCR-018) In all app interactions, communications with converted consumers, and on the website, call center must use the same name, and must be explicit about the relationship between the app vendor, the call center, and the vendors of the offers; call center must also be explicit that they may be offering additional products and services, as this is the business of the call center.
Consumers must never be confused as to the relationship between the app and the call center, and the offers and the call center. This includes affiliates, resellers, agency and BPO relationships, and subcontractors. Consumers must be reminded in each interaction that the call center's purpose is to sell them additional products and services. Greetings must be

explicit about the relationship between call center and the app vendor, even in BPO relationships.

(CCR-019) Consumers may only be offered additional products and services once they have clearly and convincingly confirmed that the purpose of their call has been fulfilled.
No offering anything until consumer has been satisfied with the reason they called: activation, support, questions, etc. Consumer must give a clear indication that they believe the intent of their interaction was satisfied. If an activation call, consumer must be fully activated before any offers are made. If a support call, consumer must be fully satisfied before any offers are made. If consumer is not satisfied, no offers must be made.

(CCR-020) Outbound interactions may only take place with consumers with existing business relationships with the call center.
No cold outbound interactions are allowed. A certified call center offers support in exchange for the right to offer upsold products and services on inbound calls. Outbound interactions are to be used only to service consumers who have converted to become a customer of the call center.

**(CCR-022) Agents must never diagnose the consumer's problem themselves on app interactions without using licensed (if applicable), consumer-available software to obtain a diagnosis. Software and its diagnosis must be disclosed during the call.
Agents/employees play the role of support and salesperson; not the role of an expert diagnostician. Software makes the diagnosis, and the diagnosis as well as the tools, must be disclosed to the consumer during the interaction and, if they convert, in the follow-up communications. If call center uses its own tools, these tools must be available for app vendor and AppEsteem to download and run and validate they are not Deceptors.

REMOTE ACCESS SESSIONS

**(CCR-023) Call center must receive explicit permission from the consumer before initiating a remote access session with the consumer's system. This must be done verbally before initiation, and once again within the remote access software. At both times, the agent/employee is to verify that the consumer does not feel under pressure.
We require a two-phase consumer consent: once verbally, and once in the remote session. This consent must be obtained without any tactics that leaves a consumer feeling pressured.

(CCR-024) Call center may only initiate a remote access session during the app interaction, and must use software administrative settings to ensure no access can be initiated outside of the app interaction.
Remote session initiations are limited to only when the call center and the consumer are interacting. This limitation overrides any "permission" the consumer may grant the call center. If the remote access software does not support features necessary to meet this requirement, that remote software must not be used. Note that the remote session can continue beyond the app interaction if the consumer gives permission.

(CCR-025) Remote access software must be enterprise-quality, fully licensed, available for inspection by the app vendor and AppEsteem, and not detected as either malware or PUP by any major antimalware vendor.
No trial-ware; no free versions. The call center is opening a connection over the internet into the consumer's system; it is the responsibility of the call center to ensure that no vulnerability is added. Home-grown tools must be available for consumer, app vendor, and AppEsteem to inspect.

(CCR-026) To protect PII and personal data, consumer must be warned, and call center must receive a clear affirmative response, that private windows are closed before remotely accessing the consumer's system.
We require the consumer is warned, and a clear response that demonstrates they understand, before the remote access starts. If the response is not clear, no remote access may be initiated.

(CCR-027) Consumers must be informed how they can disconnect any remote access session at any time.
Consumers need both the knowledge and the ability to terminate remote access sessions.

(CCR-028) Before any fixes or changes are applied to a consumer's system during an app interaction, a system restore point or backup must be done, and instructions for restoring are provided to the consumer at the time and in the email post-conversion.
The consumer must feel they are in control, and can "get out" of any situation by reversing it.

AGENTS

(CCR-029) All agents must be trained and tested at least annually on compliance and ethics, including these requirements and the intent behind them.
This is a requirement for all call center employees and agents.

(CCR-031) All offers must have well-defined, publicly published, structured pricing, including a maximum allowed price and a pre-paid or discounted service duration of no more than one year, which call center agents must not exceed to non-customers.
This is to avoid the pressure of pushing one solution above another and working instead to meet the consumer's need. Pre-paid or discounted service timeframe is limited to one year to prevent on-the-spot decision making for long-term commitments to non-customers.

CONVERSIONS

(CCR-032) All recurring fees must be disclosed and accepted verbally, and re-disclosed in an email to the consumer. If the fee includes a negative option, these must follow AppEsteem requirements on disclosure, notification, and cancellation, and must also follow any applicable government auto-renewal laws.
The intent is to prevent consumer confusion or anger when they see recurring charges in the future.

(CCR-033) Call center employees must never handle payment details outside of PCI-certified environments.
The intent is for the consumer to feel secure and in control of their data, never wondering what the agent may do with their data.

(CCR-035) Before collecting payment details from the consumer, each conversion requires the consumer to verify the payment details and any recurring charges and how they will appear, plus confirm that they understand the service is additional and not required for the product.
The goal is to ensure the consumer truly understands what they're paying for and that it's not the same product/service as the app.

(CCR-036) Consumer can cancel the purchase of additional products and services at any time within 30 days, without any requirements for one to one interaction.

We believe that knowing there is liberal return policy that doesn't require potential confrontations is a key factor to keeping consumer sentiment high.

(CCR-037) Follow-up confirmation emails must be sent to all successful conversions. The emails show details of charges and how any recurring charges will appear, which remote access software and diagnostic software was used, and how to return.
This is to ensure the consumer has records of exactly what offers they accepted and why they accepted them, as well as how to return. Diagnostic information may be provided but the diagnosis itself must not be changed. This doesn't have to be a single email.

(CCR-039) Products offered during app interactions must also meet compliance for one-to-one interactions and must not be classified by AppEsteem as a Deceptor.

Call center may not offer products that do not meet the certification standards to be in their own call center.