

Cobranded · Amazon Card

Lernübersicht – reine Session-Inhalte

Refresh Training Transcom · Zusammenfassung aller Sessions der Cobranded-Schnellreferenz. Enthält DAL-Grundlagen und Ticketdisziplin, Access/PIN/Trusted Device, Card Controls und Declined Transactions, Billing und Refunds, Fraud- und Hochrisiko-Themen sowie die finale Kalibrierung und Prüfungsstruktur.

Inhalt

- Session 1** · DAL-Grundlagen & Ticketdisziplin
- Session 2** · Access, Telefonnummer, Trusted Device, PIN
- Session 3** · Card Controls, Declined Transactions, Code K
- Session 4** · Billing, Statements, Unpaid Invoices, Refunds
- Session 5** · Fraud, Phishing, Identity Theft, Police, Death
- Session 6** · Finale Kalibrierung & Prüfungsstruktur

Hinweis: Das Cobranded-Curriculum umfasst sechs Sessions (1–6) inkl. finaler Kalibrierungs-Session.

Session 1 - DAL-Grundlagen & Ticketdisziplin

Entscheidungsbaum, Prozesswahl und vollständige DAL-Tickets

Entscheidungsbaum

DAL-GRUNDLAGEN

- 1 Self-Service möglich? → Kunde führt den Prozess selbst durch.
- 2 Kann CC die Aktion selbst durchführen? → App Action / Picaso.
- 3 Troubleshooting möglich? → durchführen.
- 4 Backoffice-Eingriff nötig? → DAL erstellen.
- 5 Technisches Problem? → Eskalation.

Prozess-Tabelle

DAL-GRUNDLAGEN

PROZESS	WER LÖST?	BEISPIEL
Self-Service	Kunde	Zugangscode ändern
App Action	Agent	Kreditlimitverringerung
Troubleshooting	Agent	Login-Problem
DAL	Backoffice	Datenänderung
Eskalation	IT / ServiceNow	Systemfehler

Kein DAL wenn

- Self-Service vorhanden ist
- Agent die Aktion selbst durchführen kann
- Problem noch nicht vollständig geprüft wurde

DAL-Codes

DAL-CODES

CODE	ZWECK
1	Kartenersatz bei Betrug in Web/App
3	Betrug (Kartensperrung nötig)
4	Streitfall / Technische Disputes
5	Geldautomaten-Disputes
9	Allgemeine Wartung/Vorfälle, PIN-Reset ohne physische Nutzung
22	Kundendaten, die der Kunde nicht selbst ändern kann (Vorname, Nachname, Geschlecht)
42	Gebühren/Provisionen, Ex-Customer Refund
55	Punkte & Bewegungen
89	Zugriffsrecht / Systemproblem bei App-Anfrage
90	Stornierung aktiver Kunden
145	Kartenanpassungen (Startgutschrift)
155	Widerspruchsrechte (GDPR)

CODE	ZWECK
157	E-Mail / Anschrift bei Fehlermeldung
187	Vulnerable Customer
190	Kartenzertifikate
296	EPP-Wartung / Ratenkauf-Fehler
303	Portabilitätsrechte (GDPR)
329	Stornierung Prospects
400	Cobranded-Phishing
14867	Telefonnummernänderung

Gutes DAL enthält

- Kundenanliegen
- Problem
- Prüfung – was wurde konkret geprüft
- Dokumente
- Erwartete Aktion

Tranxfer

Nur nutzen, wenn der Prozess es ausdrücklich verlangt oder der Kunde Dokumente technisch nicht hochladen kann.

Warum Tickets hängen bleiben

- Fehlender Ausweis / Selfie / Händlernachweis / Stornierungsbestätigung
- Unvollständige Beschreibung
- Dokumente über DAL statt über Tranxfer angefordert

Session 2 – Access, Telefonnummer, Trusted Device, PIN

Zugangscode-Recovery, Nummernwechsel und PIN-Fälle

5 Fragen bei jedem Access-Problem

ACCESS

- Kennt der Kunde den Zugangscode?
- Hat er Zugriff auf die Telefonnummer?
- Hat er Zugriff auf die App?
- Hat er den Sicherheitspin?
- Hat er ein Trusted Device?

Access Key Recovery – Reihenfolge

ACCESS

- 1 Self-Service (biometrisch, OTP + Sicherheitspin, Kartennummer + Karten-PIN) — immer erste Wahl
- 2 Kundenservice: temporärer Zugangscode, wenn alle Voraussetzungen erfüllt sind
- 3 Backoffice (Brief) — immer letzte Wahl

Temporärer Zugangscode NUR wenn

ACCESS

Anruf von der registrierten Nummer + 3 Sicherheitsfragen korrekt + Kundendaten stimmen vollständig überein.

Telefonnummer ändern

ACCESS/PHONE

SITUATION	VORGEHEN
Kunde kann selbst ändern	Kein DAL
Active Customer + technisch nicht möglich	DAL 14867
Neue Nummer + Access Key bekannt	Self-Service prüfen
Neue Nummer + Access Key unbekannt + alte Nummer verfügbar	Erst Zugangscode wiederherstellen, dann Nummer ändern
Kein Zugriff auf alte Nummer	DAL 14867 + Ausweis Vorder-/Rückseite + Selfie via Tranxfer

Trusted Device

ACCESS

- Nur ein Mobiltelefon möglich
- Nur ein Gerät gleichzeitig
- Verwaltbar über App → Profil → Sicherheit und Zugangscodes → Geräte verwalten

3D Secure

ACCESS

Zusätzliche Authentifizierung bei Onlinekäufen. Bestätigung per SMS oder App.

PIN-Fälle

ACCESS

FALL	VORGEHEN
PIN vergessen	Standardprozess zuerst
Nach 3 Fehlversuchen gesperrt	Prüfen, ob normaler Reset möglich ist – wenn ja: kein DAL, wenn nein: DAL 9
Grundregel	First Option immer Self-Service, Fallback: Agent Action → Troubleshooting → DAL → Eskalation

Session 3 – Card Controls, Declined Transactions, Code K

Kartencodes, Ablehnungslogik und Fraud-Block-Freigabe

Card Controls

- Bargeldabhebungen, Bezahlungen im Geschäft, Online-Zahlungen – je separat aktivierbar
- Standortkontrolle (Länder / Kontinente)
- Gilt NICHT für Online-Shops und Abonnements

Karte temporär ausschalten

Online, POS und Geldautomat funktionieren nicht, Kartendaten bleiben gleich, jederzeit wieder einschaltbar. Coaching: zuerst prüfen, ob versehentlich ausgeschaltet (Code S).

Declined Transaction – Prüfreihefolge

DECLINED TRANSACTIONS

- 1 Kartencode
- 2 Card Controls
- 3 Limit
- 4 Redsys
- 5 ZEUS
- 6 Declined Code

Kartencodes

CARD CODES

CODE	BEDEUTUNG
A	Freiwillig storniert
C	Systemstorno
S	Karte ausgeschaltet
K	Temporäre Redsys-Sperre
R	Gestohlen
L	Verloren
P	Unbezahlt
G	Gesperrt wegen offener Rechnungen

Code K Logik

CODE K

Redsys Alert vorhanden? Ja → Redsys-Prozess. Nein → DAL 42. Vor Freigabe bestätigt der Kunde die letzten 2-3 Käufe (Händler + Betrag).

ZEUS

CODE K

Zeigt, warum eine Transaktion als Betrugsverdacht markiert wurde (Fraud Codes, Ablehnungsgründe).

Declined Codes

DECLINED TRANSACTIONS

CODE	URSACHE	AKTION
206	PIN gesperrt	Zurücksetzen, keine Ersatzkarte
121	Limit	Prüfen
184	Falsche PIN / CVV	Erneut versuchen
125	Nicht aktiviert	Aktivieren
190	Sicherheitsmaßnahme	Redsys prüfen
195	Zusätzliche Authentifizierung	3D Secure / Trusted Device

Lost / Stolen / Found

FALL	VORGEHEN
Verloren + Zugangscode vorhanden	Endgültig sperren, neue Karte, Fraud Check
Ohne Access Key	Sofort an STF
ATM retained	Endgültig sperren, "Verloren" wählen, neue Karte automatisch (7 Werktage)
Dritte findet Karte	Kartenummer aufnehmen, in Redsys suchen, mit N3 blocken, Finder soll vernichten, Kunde kontaktieren, Fraud Check, Ersatzkarte anbieten

Ersatzkarte ja / nein

ERSATZKARTE JA	ERSATZKARTE NEIN
Verloren	PIN-Problem
Gestohlen	CVV-Problem
ATM-retained	Trusted Device Problem
Found Card	Temporärer Redsys Block
Fraud Block mit Ersatz	—

Session 4 – Billing, Statements, Unpaid Invoices, Refunds

Zahlungsarten, Lastschrift-Retry und DAL 42 Routing

Zahlungsarten

BILLING

ART	DETAIL
Vollzahlung	Gesamter offener Betrag
Teilzahlung fest	25 / 50 / 100 / 150 €
Teilzahlung Prozent	3 / 5 / 10 / 15 %
Mindestzahlung	Immer 25 €

Lastschrift

FAILED DIRECT DEBIT

- Einzug ca. 5 Tage nach Ausstellungsdatum
- Bleibt aktiv, auch wenn der Kunde bereits überwiesen hat
- Retry automatisch 2 Tage nach dem ersten Versuch

Kartenstatus bei offener Rechnung

FAILED DIRECT DEBIT

STATUS	FOLGE
Unter 90 Tage überfällig	Temporär gesperrt
Über 90 Tage (Charge Off)	Dauerhaft gesperrt
Nach Zahlung	Karte bis zu 5 Tage noch gesperrt

Statement Dispute vs. Transaktionsdispute

Statement Dispute = Fragen zur Rechnung. Transaktionsdispute = bestimmte Transaktion anfechten → DAL 4 / Dispute Workflow. Nicht derselbe Prozess.

DAL 42 – wann und wann nicht

DAL-CODES

WANN	NICHT
Gebühren-/Provisionsbeschwerden	Normale überfällige Rechnung
Positive Salden nach Kündigung	Fehlgeschlagene Lastschrift ohne Prüfung
Ex-Kunden-Rückerstattung	Reguläre Disputes
—	Standard-Rückzahlungen
—	Blockierte Karten durch Code K

Ex-Customer Refund

- 1 Händlername, Betrag, vollständiger Name, Geburtsdatum, E-Mail, Telefonnummer sammeln
- 2 An TL / TM weiterleiten
- 3 DAL 42 erstellen

Niemals versprechen

- Sofortige Entsperrung
- Lastschrift stoppen
- Zahlung heute sichtbar
- Automatische Rückerstattung
- Garantierte Bearbeitungszeit

Session 5 – Fraud, Phishing, Identity Theft, Police, Death

Die sensibelsten Prozesse – hier ist kein Fehler erlaubt

4 Fälle unterscheiden

IDENTITY THEFT

FALL	MERKMAL	VORGEHEN
Betrug	Kunde erkennt Transaktion nicht	"Problem melden" / Karte sperren (1 Transaktion) oder Karte sperren + DAL 3 + Polizeianzeige (mehrere)
Phishing	Kontoinhaber echt, Daten manipuliert, Zugang verloren	DAL 400, Karte sperren, Polizeianzeige
Identitätsdiebstahl	Jemand beantragt Karte im Namen des Kunden	Polizeianzeige prüfen, Karte sperren, DAL 3 Supervisor Access, Kommentar "IDENTITY THEFT"
Datenänderung	Kunde will eigene Daten ändern	DAL 22 / 157 / 14867

Identitätsdiebstahl – Pflichtdokumente (via Tranxfer)

IDENTITY THEFT

- Polizeianzeige
- Ausweis Vorder- und Rückseite
- Selfie mit Ausweis

Phishing – Ablauf

PHISHING

- 1 Vollständigen Namen, Customer ID, Telefonnummer, E-Mail sammeln
- 2 Prüfen, ob Daten geändert wurden oder unautorisierte Transaktionen vorliegen
- 3 Karte sperren
- 4 DAL 400 erstellen
- 5 Kunde zur Polizeianzeige auffordern

Police – Golden Rule

POLICE

NUR offizielle schriftliche Kanäle; telefonische Anfragen werden nicht bearbeitet. Niemals herausgeben: Geburtsdatum, Ausweisnummer, Adresse, weitere personenbezogene Daten. Nicht bestätigen: Kundendaten, Kontostatus, Umsatzinformationen.

Death Cases – Dokumentenmatrix

DEATH CASES

ANRUFER	DOKUMENTE
Vollmacht	Sterbeurkunde + Vollmacht
Erbe	Sterbeurkunde + Erbschein/Testament + Ausweis
Testamentsvollstrecker	Sterbeurkunde + Vollstreckerzeugnis + Ausweis
Nachlasspfleger	Sterbeurkunde + Bestallung + Ausweis

Death Cases - Tonalität

DEATH CASES

Immer Empathie zeigen: "Mein herzliches Beileid."

Session 6 – Finale Kalibrierung & Prüfungsstruktur

Prüfungsaufbau, Full-Score-Themen und Abschluss-Checkliste

Prüfungsstruktur

30 Fragen = 10 Fakten + 10 Prozess/Code/Routing + 10 Szenarien. Bestehensgrenze 85 % (26/30).

Die 7 Mandatory Full-Score Topics (100 % erforderlich)

- Identity Theft
- Phishing
- Police Contact
- Death Cases
- Access / Phone Number Change
- Denied Transaction Code K
- Failed Direct Debit / Blocked Card

Case Studies müssen enthalten

- 1 Checks
- 2 Aktion
- 3 Kundenformulierung
- 4 Eskalation