Fintech Customer Support Compliance Checklist

Use this checklist to ensure your support operations, tools, and workflows meet fintech regulatory standards without compromising customer experience.

1. Identity verification and KYC controls

☐ Customer identity is verified before accessing account-specific data
☐ KYC documents are stored securely and access is role-restricted
☐ High-risk customers trigger enhanced verification workflows
☐ Support agents can view verification status without exposing raw documents
☐ All identity verification actions are logged for audits

2. AML and financial monitoring

☐ Customers are screened against sanctions and watchlists
☐ Suspicious transactions are flagged automatically
☐ Support agents follow “no-tipping-off” guidelines
☐ AML escalations follow predefined workflows
☐ AML-related actions are traceable and reportable

3. Data privacy and security (GDPR / Regional Laws)

☐ All customer communications use secure, encrypted channels
☐ Sensitive data is masked or redacted inside tickets
☐ Access to PII is limited by role and context
☐ Data retention and deletion policies are enforced automatically
☐ Suspected data breaches are logged and escalated immediately

4. Support access and permission management

☐ Agents only see the data required to resolve the issue
☐ Role-based access controls are enforced by the system
☐ Temporary access is reviewed and revoked
☐ Admin actions require approval and logging
☐ Historical access can be audited at any time

5. Complaint and dispute handling

☐ All complaints are logged in the support system
☐ Regulated complaints are tagged and escalated
☐ Customers receive clear timelines and updates
☐ Resolution steps are documented for audits
☐ Root-cause trends are tracked and reviewed

6. Fraud prevention and account protection

☐ Identity is reverified before sensitive account changes
☐ Multi-step verification is enforced for risky actions
☐ Social engineering attempts are recognized and reported
☐ Fraud incidents follow defined escalation paths
☐ All fraud-related actions are auditable

7. Audit readiness and regulatory reporting

☐ Support actions are fully logged with timestamps
☐ Audit trails cannot be altered or deleted
☐ Reports can be generated without manual work
☐ Regulatory incidents are reported within deadlines
☐ Evidence is centrally stored and review-ready

If most items are left unmarked on this list, then your operations may be exposed to regulatory fines and reputational risk