3DS Authentication Implementation Checklist

Phase 1: Preparation and Partnership Setup

- [ ] Choose a payment provider certified for both **3DS 2** and **3DS 1** to handle **global transactions**.
- [ ] Confirm your chosen partner offers a **liability shift benefit** upon successful 3DS authentication.
- [ ] Decide between implementing a **Hosted Payment Page** (fast setup) or a **Direct API/SDK integration** (custom UI control).
- [ ] Integrate your payment partner's mobile **SDKs** (iOS/Android) if you sell video games or SaaS via mobile apps.

Phase 2: Data Implementation and Setup

- [ ] Ensure your checkout captures and transmits **mandatory customer data fields** (email, billing address, IP address) for all transactions.
- [ ] Integrate **contextual data points** from your user database (e.g., customer account age, purchase history) into the payment request to enable frictionless flow.
- [ ] Verify that your system can receive and process the **Authentication Value (CAVV)** from the 3DS process to prove validation.

Phase 3: Strategy and Exemption Configuration

- [ ] Set up your system to trigger the "**Challenge Flow**" only when mandated by **SCA rules** (EEA cards exceeding exemption limits) or when fraud risk is high.
- [ ] Configure logic to automatically request the "**Frictionless Flow**" for all low-risk, trusted, and non-EEA card transactions.
- [ ] For SaaS subscriptions, flag the initial payment as requiring 3DS to establish the **Stored Credentials** framework.
- [ ] Automate the "**Recurring Payment**" exemption flag for subsequent fixed-amount subscription renewals to bypass re-authentication.
- [ ] Establish a mechanism to perform soft **re-authentication checks** for annual SaaS subscriptions to maintain Stored Credential validity.

Phase 4: Testing and Optimization

- [ ] Conduct **end-to-end testing** using card numbers provided by your payment partner to simulate both frictionless and challenge flows.
- [ ] Test the checkout experience across major browsers and mobile operating systems to confirm the authentication prompt appears correctly without redirects.
- [ ] Monitor transaction **authorization** rates and **chargeback** rates post-launch to confirm the expected decrease in fraud liability.
- [ ] Use **A/B testing** on checkout pages to ensure any necessary **Challenge Flow** screen minimizes customer abandonment.