Article 91: Strong customer authentication

Council first-reading position 8543/1/26 REV 1, 4 November 2026. Verified 19 November 2026. Final wording and numbering may change.

Application
The Council position provides for general application 21 months after eventual entry into force under Article 124. Final Official Journal text and calendar dates remain to be checked.

Provision
Article 91(1)-(10)

Requirement
Providers apply strong customer authentication to online account access, electronic payment orders and risky remote actions, including specified token, limit, password and contact-information changes. The article distinguishes recipient-initiated transactions, remote mandate setup, direct-debit mandates and mail or telephone orders. Remote payment orders require dynamic linking; specified proximity payments require dynamic linking or security measures of identical effect. Credentials must be protected and exemptions remain optional.

Responsible
The payment provider applies the relevant authentication and credential controls. EBA develops exemption standards under Article 97 and the paragraph 10 guidelines; the national authority receives the required demonstration for the two-inherence derogation.

Timing
Authentication is required at the relevant access, order or action. EBA guidelines for assessing independence of two inherence elements are due by 18 months after eventual entry into force.

Conditions and exceptions
The usual elements belong to different categories. The two-inherence derogation requires demonstrated independence at all times and high security. Recipient-initiated payments without payer interaction are distinguished from remote mandate setup. Mail and telephone orders require the stated security requirements and checks.

PSD2 comparison
PSD2 Articles 97(1)-(3), 98(3). The Council correlation is an article-level starting point, not equivalence of every duty.

Source: Council of the European Union, 8543/1/26 REV 1. Updated article card.

What it means for the fraud function

- Map every account-access, payment and high-risk profile-change journey to its precise trigger.

- Retain the reason and selecting party for exemptions and review their risk assumptions.

- Assess authentication evidence separately from consent and from liability under Articles 56 and 63.

Common misreadings

- Authentication success does not itself prove that a transaction was authorised.

- An available exemption does not oblige the provider to use it.

Episodes: Coverage follows the curriculum. Links on the updated HTML card.