**Amendment of the German Asociation of Corporate Treasurer with regard to SCA**

**(Strong Customer Authentication)**

SCA in the process with consumers is excellent to protect against Fraud.

**Application in Businesses / Treasury**

In the corporate environment, too, strong customer authentication of users for online payments must be guaranteed, which is achieved through two-factor authentication (2FA). When using electronic banking tools (whether through service providers such as TIS or banking products such as Deutsche Bank AG's db-direct internet or Commerzbank's GPP Global Payment Plus), tokens/apps are used to generate a session key or QR code within the scope of the user's login by means of user ID and password.

This mandatory requirement (2FA) is also/especially used in conjunction with a corporate seal. In this case, a contract is concluded between the bank and the corporate which obliges the corporate to comply with SCA and, in particular, to check the identity of the user (staff) in the same way as the bank itself would have to do for the onboarding/KYC of a customer within the framework of the requirements of the Money Laundering Act, the German "Abgabenordung" etc. The advantage of the "Corporate Seal" is that the authorised signatory users do not have to be "onboarded" (accessory) with the bank. However, the bank has the right to request the names of the authorised signatories at any time (declaratory). In day-to-day business, the bank does not know which users have authorised payments. All payment orders received by the bank are considered sufficiently authenticated by the corporate seal and the upstream 2FA. The bank thus relies on "the good company". SWIFT works according to the same principle with its bank members or with authorised corporates that use the SWIFT network for messaging within SCORE. Here, too, no bank receives the name of a principal, neither from bank members nor from corporates. The "seal" is the key to ensuring that only trusted members are connected to the SWIFT network and that users can remain anonymous.

The possibility of agreeing on a "Corporate Seal" between Corporate and the bank makes it much easier to change authorised signatories within the company without the bank being involved in the verification obligation and without the authorised signatory (user) having to be recorded in the banking systems (KYC). This increases efficiency between the bank and the corporate without violating legal requirements.

However, for anti-money laundering reasons, the Norwegian legislator requires that the name and national ID (or a comparable feature in the case of foreign authorised signatories) of the bank must be provided for all transactions on bank accounts held in Norway, regardless of whether a corporate seal has been agreed between the bank and the corporate or whether the bank is already aware of the authorised signatories through KYC/onboarding.

This requirement of the Norwegian regulator makes the use of a corporate seal "absurd".

There is a concern among treasurers that the achievements of efficient payment transactions from central corporate units (payment factories, central treasury or shared service centres) with banks will be destroyed due to analogous national legislation also on EU territory.