Danish FSA clarifies requirements related to strong customer authentication procedures

Martin Christian Kruhl
Partner, PhD

In July 2020, the Danish Financial Supervisory Authorities ("DFSA") conducted an inspection on the business premises of Nets A/S ("Nets"), the largest payment service provider in Denmark, to assess Nets' use of strong customer authentication in connection to its provision of payment services.

In a summary of the report following the inspection, which has been published on the DFSA's official website, the DFSA elaborated on how the specific requirements related to strong customer authentication under the Danish Payment Act are to be understood. More specifically, the DFSA commented on three distinct authentication issues, which are the subject of this newsletter.

Legal setting

The Danish Payment Act implements the second Payment Services Directive, commonly referred to as PSD2.

According to the Danish Payment Act, a payment service provider is obliged to ensure that payment transactions can only be initiated and completed by applying strong customer authentication.

Strong customer authentication is also known as two-factor authentication and requires that the payer proves his/her identity through the use of two or more independent elements. The independent elements must be

either *knowledge* (e.g. a password), *possession* (e.g. a debit card) or *inherence* (e.g. voice recognition). Thus, two independent elements could constitute of the combination of a password and a one-time password made available to the customer via a phone or another mobile device.

The DFSA's clarifications

#1 – Unmanned terminals

Firstly, the DFSA explains why the performance of payment services via unmanned terminals, such as parking meters and bus ticket machines, will often require the use of strong customer authentication.

The DFSA stated that a payment service provider *can* omit from performing strong customer authentication in situations where the payer is purchasing a transport fare or a parking fee; however, this requires that the payment service provider is able to identify the transaction as such in its own system. If a provider is unable to make such identification, the provider is required to conduct strong customer authentication.

#2 – Sole use of chip

Secondly, the DFSA noted that a payment provider is prohibited from carrying out payment transactions in situations where payment can be made via a purchase terminal using only the chip in the credit card, i.e. without requiring a password or any other form of "knowledge" element.

#3 – Magnetic stripes as an element of possession

Finally, the DFSA presented its view on the use of a magnetic stripe as an element of possession in the strong customer authentication process.

The DFSA found that a magnetic stripe is – in its current state – unfit to serve as an element of possession, because a magnetic stripe can – by relatively simple means – be either copied or recreated.

As the magnetic stripe does not suffice as an element of possession, payments which are performed by the use of a magnetic stripe combined with a password will not be considered two-factor authorised.

Services	Regulatoriske forhold i den finansielle sektor, International handel, investeringer, reguleringer og compliance, FinTech
Sectors	Financial Services