JONES DAY

COMMENTARY

MARCH 2018

EU Regulatory Technical Standards for Strong Customer Authentication Enter Into Force

IN SHORT

The Situation: The second EU Payment Services Directive requires banks to give third-party payment service providers ("TPPs") access to the bank accounts of their customers (with their consent), in order to enable TPPs to provide account information and payment initiation services.

The Result: The regulatory technical standards ("RTS") on strong customer authentication and secure standards of communication lay down minimum requirements for the interfaces between banks and TPPs.

Looking Ahead: The RTS ban traditional "screen scraping". Banks that make available a dedicated interface for account access by third-party service providers will also be allowed to block forms of "screen scraping", whereby a TPP identifies itself to the bank. Nevertheless, even banks that make available a dedicated interface must allow "screen scraping" as a contingency measure.

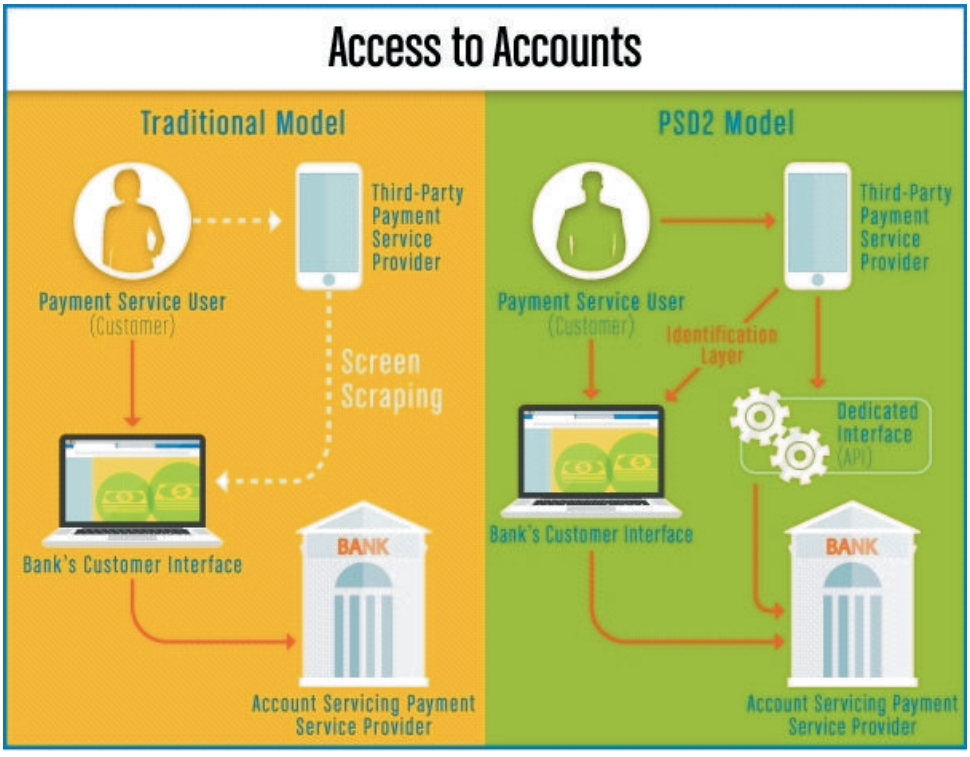
SKIP TO THE FULL VERSION.

On March 14, 2018, the regulatory technical standards for strong customer authentication and common and secure open standards of communication entered into force. The obligations set forth in these RTS will apply after a transitional period of 18 months, on September 14, 2019.

The RTS were developed by the European Banking Authority ("EBA") on the basis of a mandate in the revised Payments Services Directive ("PSD2").

In February 2017, the EBA submitted draft RTS for adoption to the European Commission. However, the Commission disagreed with parts of the EBA's draft and, in a controversial move, decided to amend it. The Commission finally adopted its amended version on November 27, 2017.

After a three-month period for review by the European Parliament and the Council, the RTS have now been published in the *Official Journal* of the European Union and have entered into force.



The RTS mainly set out minimum requirements in relation to strong customer authentication ("SCA") and the interfaces for third-party access to the accounts. "SCA", as defined by PSD2, means (at minimum)

two-factor authentication—authentication based on two or more of the following elements:

- knowledge (something the user *knows*—for example, a password or a PIN),
- possession (something the user *owns*—for example, a card or smartphone), and
- inherence (something the user *is*—for example, a fingerprint or iris scan).

The RTS provide for several exemptions from the obligation to use SCA, e.g., for contactless payments and low-value transactions (with limits on the amounts and the number of consecutive transactions). An additional exemption is for electronic payment transactions initiated through processes or protocols that are made available only to payers who are not consumers. However, payment service providers must cease to make use of the exemptions if the monitored fraud rate exceeds certain thresholds.

The interface between banks and TPPs is probably the most controversial aspect of the RTS. Currently, TPPs commonly use a technique called "screen scraping" to access bank account information and initiate payments. This means accessing the accounts through the customer interface using the customer's security credentials. Banks sought a ban on this practice, while fintech companies favored allowing it at least as a fallback solution.

The RTS confirm that traditional screen scraping, whereby the TPP impersonates the customer and thus has access to all the customer's data without identifying itself to the bank, will be banned after the 18-month transitional period. However, screen scraping is not completely dead. Banks can comply with the obligation to open up their accounts to TPPs in two ways, either: (i) by making available a dedicated interface (an application programming interface or "API"); or (ii) through the customer interface. The latter is basically screen scraping, except that an identification layer for TPPs would be added to the customer interface.

The interface between banks and third-party payment service providers is probably the most controversial aspect of the regulatory technical standards.

In addition, the RTS require banks that opt to use APIs to have contingency measures in place in case of an unplanned unavailability of the interface or a systems breakdown (presumed in the absence of reply within 30 seconds to five consecutive requests), which is again accessed through the bank's customer interface (i.e., screen scraping).

The competent national authorities may exempt banks from the obligation to have a fallback mechanism in place if they can demonstrate that their dedicated interfaces are sufficiently robust. However, such exemption can be revoked if the conditions are no longer met. In that case, banks have to make available the contingency measure within two months.

The RTS' fallback mechanism provision may mean that banks opting for APIs must develop both a dedicated interface *and* an identification layer for direct access using the customer interface. This may be necessary *even if* national authorities grant an exemption from the fallback mechanism, since developing an identification layer for TPP access would not be practicable within the above-mentioned two-month period.

Although the obligation to make available either a dedicated interface or a TPP identification layer in the customer interface will apply only after the transitional period of 18 months, in practice, banks must be ready in 12 months, as the RTS provide that banks have to make available interface documentation as well as a testing facility no later than six months before the RTS' application date.

There is currently no EU-wide standard for PSD2-compliant access-to-the-account APIs. However, there are standardization initiatives at national or regional level (e.g., Open Banking UK and the Berlin Group). The complexity of connecting banks and TPPs also creates business opportunities for providers of "aggregator" services.

The text of the RTS is available here. The European Commission has also published a fact sheet concerning the RTS.

FIVE KEY TAKEAWAYS

1. The RTS' requirements regarding SCA and interfaces for third-party access to the accounts will become effectively applicable after a transition period of 18 months, on September 14, 2019.
2. The RTS provide for several exemptions from the general obligation to use SCA, but these can be lifted if monitored fraud rates exceed certain thresholds.
3. For third-party access to bank accounts, traditional screen scraping will be banned. However, banks must still enable a form of screen scraping whereby TTPs identify themselves as such, either as the main solution for access to the accounts or as a fallback mechanism.

WANT TO KNOW MORE?
READ THE FULL VERSION.

CONTACTS


Philippe Goutay
Paris


Olivier Haas
Paris


Alexandre Verheyden
Brussels

4. Banks must be ready with the development of the interfaces for third-party access within 12 months, to give TPPs time to integrate the banks' APIs by September 2019.

5. In the absence of an EU-wide API standard for PSD2, reducing the complexity of connecting banks and TPPs will largely depend on national or regional standardization initiatives and providers of "aggregator" services.

Karl Stas
Brussels

YOU MIGHT BE INTERESTED IN: **Go To All Recommendations >>**

Belgium Launches Consultation Process on EU Prospectus Regulation

The European Securitisation Regulation: The Countdown Continues...

French Regulators Launch Public Consultation for Initial Coin Offerings

---

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a legal institution with more than 2,500 lawyers on five continents. We are One Firm Worldwide℠.