



Herausforderungen der PSD2 *Mehr Komfort, mehr Sicherheit* *Ein Überblick der Änderungen für Institute und Kunden*

Themenbereich: Digitale Finanz-Plattform

Messe-Stand: FP07

Fragen beantwortet
 Ihnen Ihre zuständige
 Kundenberatung.

Die Umsetzungen der Payment Service Directive 2 (PSD2) soll die Sicherheit im Zahlungsverkehr erhöhen und regelt den Zugang dritter Zahlungsdienstleister neu. Ein Regulatory Technical Standard (RTS) regelt die Anforderungen an die Schnittstelle für Drittdienstleister sowie die starke Kundenauthentifizierung (Strong Customer Authentication – SCA). Mit der Veröffentlichung im März 2018 ergibt die 18-monatige Umsetzungsfrist den Stichtag 14.09.2019. Neben diesen Anforderungen müssen durch weitere veröffentlichte Guidelines beispielsweise auch Anforderungen an das Fraud Reporting umgesetzt werden.

Damit Sie PSD2 in den Instituten erfolgreich umsetzen, werden Sie sowohl durch die Sparkassen-Verbände u.a. durch einen Rollout-Leitfaden für strategische Entscheidungen und deren Umsetzung unterstützt als auch durch die Finanz Informatik durch Rundschreiben und Administrationshilfen.

Neue Pflichten und Ausnahmemöglichkeiten bei der starken Authentifizierung

Die Umsetzungen des RTS werden sowohl Auswirkungen auf Kunden als auch auf die Institute haben. Kunden müssen sich künftig beim Zugriff auf Kontoinformationen immer stark authentifizieren. Als definierte Ausnahme kann auf die SCA verzichtet werden, sofern innerhalb der letzten 90 Tage eine SCA durchgeführt wurde und auf Umsätze der letzten 90 Tage zugegriffen wird.

Auch für Transaktionen werden weitere Ausnahmen der SCA umgesetzt. Diese können je nach Administration des Instituts und Wunsch des Kunden genutzt werden. Sie beinhalten beispielsweise Whitelists, Zahlungen an sich selbst, Kleinstbetragszahlungen sowie die Transaktionsrisikoanalyse (TRA).

Die genannten Funktionen werden künftig sowohl bei der neuen Drittdienste-Schnittstelle als auch in der Internet-Filiale via FinTS bzw. der S-App greifen. Eine zentrale Komponente übernimmt künftig die Prüfung, ob ein eingereicherter Zahlungsauftrag stark authentifiziert werden muss oder nicht.

Bitte umdrehen >>



Seite 02

Transaktionsrisiken im Blick und Betrug zuverlässig erkennen

Die TRA wird durch neue Anwendung »TANja« unterstützt. Diese prüft gemäß PSD2 vorgesehene Kriterien (z. B., ob die vom Kunden genutzten Geräte durch Malware kompromittiert sind oder die Zahlung von einem unüblichen Ort ausgelöst wird) und entscheidet, ob die Zahlung ohne TAN ausgeführt werden darf (gemäß PSD2 bis maximal 500,- EUR). Maßgeblich für die Nutzung zur Ausnahme der TRA ist die Betrugsrate des Instituts, welche aufsichtsrechtlich definierte Grenzwerte nicht überschreiten darf. Mit der neuen Anwendung »Betrugsrate im Zahlungsverkehr« (BRZV) stellen wir Ihnen neben der Betrugsrate selbst auch transparente statistische Daten zur Verfügung. Mit deren Hilfe können neben den Anforderungen der PSD2 auch Maßnahmen zur Reduzierung von Betrugsfällen und damit zur Steuerung der Betrugsrate eingeleitet werden.

Eine wichtige Maßnahme zur Optimierung der Betrugsrate stellt die Phishing-Prävention (PPZV) dar. PPZV identifiziert prüfungsrelevante Zahlungsvorgänge der einzelnen Zugangswege und somit auch künftig die mit PSD2 verbundenen Zahlungsauslösdienste. Im Rahmen des Compliance-Prüfservice (CoP) stehen Ihnen administrierbare Regeln zur Verfügung – zur Anpassung an aktuelle Bedrohungsszenarien und auch im Sinne der effizienten Bearbeitung zur Abgrenzung von Verdachtsfällen.

Fazit

Die mit PSD2 umzusetzenden Ausnahmen einer starken Kundenauthentifizierung ermöglichen dem Kunden mehr Komfort und Sicherheit bei Kontozugriffen und Zahlungstransaktionen. Die Anwendungen der FI in der ZV-Risikosteuerung bieten Ihnen die Möglichkeiten, Ihre Kunden im Rahmen der Online-Kontoführung sicher und intelligent zu schützen. Für die erfolgreiche Umsetzung der PSD2 in den Instituten erhalten Sie entsprechende Unterstützung durch die Sparkassen-Verbände und die Finanz Informatik.

Fragen beantwortet
Ihnen Ihre zuständige
Kundenberatung.