A&L Goodbody

FINANCIAL REGULATION ADVISORY

PSD3 and PSR:

What FinTechs, Payment Institutions, EMIs and OEMs need to know

algoodbody.com

A&L Goodbody

CONTENTS

01 / AT A GLANCE

The final compromise texts of the third Payment Services Directive (**PSD3**) (see here) and the Payment Services Regulation (**PSR**) (see here) represent the most significant overhaul of the EU's payments regulatory framework since the second Payment Services Directive (**PSD2**) entered into force in 2018.[1]

Together, these legal acts will reshape the landscape for FinTech firms such as payment institutions, electronic money institutions (**EMIs**), payment initiation service providers (**PISPs**), account information service providers (**AISPs**) and technology companies, including original equipment manufacturers (**OEMs**) of mobile devices. This article examines the key reforms under PSD3 and PSR and outlines the practical implications for FinTechs and how they should prepare.

1 *Article references in this document refer to provisions in the final compromise texts of PSD3 / PSR.*

02 / KEY TAKEAWAYS

For EMIs:

The standalone authorisation for EMIs is being abolished. EMIs must transition to a new unified payment institution regime under PSD3 within 27 months of entry into force, with lower initial capital (€250,000 for e-money issuance). Failure to comply within the transitional window results in automatic suspension from providing payment services.

For Payment Institutions:

Initial capital thresholds have increased for most services (€150,000 for core services, €40,000 for money remittance), with a cumulation rule for firms offering multiple service types. Own funds must now be calculated using Method B by default. Safeguarding obligations are strengthened with new transparency, concentration risk and winding-up plan requirements. Transaction monitoring is now mandatory on both payer and payee sides, with direct liability for non-compliance.

For PISPs and AISPs:

The open banking framework has been substantially overhauled in their favour, as dedicated application programming interfaces (**APIs**) are now the default access route for AISPs and PISPs, the data parity principle is enhanced and twelve specific prohibited obstacles are now listed in the legislation. However, a new consent dashboard gives users an easy route to revoke access. AISPs benefit from a relaxation of strong customer authentication (**SCA**) rules (first-access only by the account servicing payment service provider (**ASPSP**)) but now bear the 180-day re-authentication obligation themselves.

For OEMs and Tech Companies:

A fair, reasonable and non-discriminatory (**FRAND**) access obligation requires mobile device manufacturers and electronic communications service providers to grant payment service providers (**PSPs**) interoperability with near-field communication (**NFC**), secure elements and other payment-critical hardware and software features. General conditions of access must be published. Telecoms providers also face new obligations to combat spoofing and to cooperate with PSPs on fraud data exchange.

For all FinTechs:

The enforcement regime is significantly strengthened, with maximum fines of 10% of annual net turnover for legal persons (a maximum fine of up to 10% of turnover is already provided for under the Central Bank of Ireland's administrative sanctions regime). Mandatory fraud information sharing arrangements must be joined. The impersonation fraud liability regime creates a new refund obligation where the PSP's own communication channels are spoofed. New regulatory technical standards (**RTS**) will replace the existing RTS in Commission Delegated Regulation (EU) 2018/389 (**SCA RTS**) to recalibrate SCA exemptions, potentially with differentiated thresholds for consumer and non-consumer transactions.

Timeline:

21 months from entry into force for transposition and application (27 months for payee verification). Firms should begin gap analysis immediately to identify the operational, governance and compliance changes needed well ahead of implementation.

03 / THE END OF THE EMI AS A SEPARATE CATEGORY

The most structurally significant change in PSD3 is the merger of the EMI and payment institution authorisation regimes into a single framework. PSD3 will repeal both PSD2 and the E-Money Directive (Directive 2009/110/EC) (**EMD2**) and will absorb the latter's provisions (Article 48 PSD3), meaning that the standalone EMI authorisation will cease to exist. Existing EMIs will need to transition to authorisation as payment institutions under PSD3, with e-money issuance reclassified as a payment service listed at point (8) of Annex I to PSD3 (Articles 1 and 2 PSD3).

This has several practical consequences. Firms currently authorised as EMIs will need to comply with the transitional provisions in Article 45 of PSD3, which afford a window of 21 months from entry into force to continue operating under existing authorisations, followed by a further 6-month period within which competent authorities must verify compliance with the new framework (Article 45(1) and (2) PSD3). Competent authorities may grant automatic authorisation where they already have evidence of compliance (Article 45(3) PSD3), but firms should not assume this will be the case. A failure to meet the new requirements within the transitional window will result in suspension from providing payment services (Article 45(2) PSD3). Competent authorities may exceptionally extend the deadline by up to three months where they have not been able to process the information provided in time (Article 45a PSD3).

For FinTechs that have built their business models around e-money issuance, including many digital wallet providers, prepaid card programmes and e-money token issuers, the practical impact will be felt in the need to re-examine their regulatory permissions, capital requirements and safeguarding arrangements against the PSD3 framework.

04 / HIGHER CAPITAL REQUIREMENTS AND A NEW OWN FUNDS METHODOLOGY

PSD3 amends the initial capital thresholds for payment institutions, reflecting the fact that these had not been adjusted since 2007 (Article 5 PSD3). Payment institutions providing services under points (1) to (5) of Annex I (i.e. account services, payment execution, issuing, acquiring and money remittance) must now hold initial capital of at least €150,000 (up from €125,000 under PSD2). Money remittance-only providers face a new minimum capital threshold of €40,000 (up from €20,000 under PSD2), while the payment initiation services threshold remains unchanged at €50,000. For firms providing the new e-money service under point (8) of Annex I, initial capital of at least €250,000 is required (down from €350,000 under EMD2). Importantly, where a payment institution provides services falling under more than one of these categories, the minimum amounts must be added together. This cumulation rule will particularly affect FinTechs with diversified service offerings.

Payment institutions that both issue e-money and provide other core payment services must hold own funds equal to the sum of the requirements calculated under Method B (or A or C, as applicable) for payment services (Article 7(2) PSD3) and Method D for e-money issuance (Article 8(4) PSD3).

The own funds calculation methodology itself has been tightened. Competent authorities must now require payment institutions to apply Method B (based on payment volume) by default, with Methods A and C available only where a competent authority determines that the institution's business model involves a small number of high-value transactions (Article 7(2) PSD3). The European Banking Authority (**EBA**) is mandated to develop RTS specifying the criteria for such business models (Article 7(6) PSD3). This will reduce the supervisory discretion that previously existed, providing greater consistency across Member States.

05 / ENHANCED SAFEGUARDING OBLIGATIONS

PSD3 significantly strengthens the safeguarding regime for payment institutions (Article 9 PSD3). The core requirement remains that all funds received from payment service users must be either ring-fenced from the institution's own funds or covered by an insurance policy or comparable guarantee (Article 9(1) PSD3). However, several important enhancements have been introduced.

Payment institutions must now inform their users, in a clear and transparent manner, of how funds are safeguarded, which Member State's insolvency law applies, and in which Member State a claim should be raised in the event of insolvency (Article 9(1), sixth subparagraph, PSD3). This transparency obligation reflects concerns that payment service users, whose funds, unlike bank deposits, are not covered by deposit guarantee schemes, may not understand the protections (or lack thereof) available to them.

The safeguarding provisions also now explicitly accommodate funds held in settlement accounts with designated payment systems under the Settlement Finality Directive (Directive 98/26/EC) (Article 9(1a) PSD3). Such funds will be considered compliant with safeguarding requirements provided they are not commingled with funds of persons other than payment service users and are ultimately held with credit institutions or central banks. Concentration risk must also be avoided, and payment institutions must endeavour not to safeguard all funds with a single credit institution (Article 9(2) PSD3).

Furthermore, applicants intending to apply for authorisation for services listed at points (1) to (5) and point (8) of Annex I must now submit a winding-up plan as part of their application, adapted to their envisaged size and business model, including arrangements for the return of safeguarded funds in the event of a disorderly wind-up (Article 3(3)(s) PSD3). This is a new requirement that will demand careful planning from FinTechs seeking authorisation.

The EBA is mandated to develop RTS on safeguarding risk management frameworks, including requirements on segregation, designation, reconciliation and calculation of safeguarded funds (Article 9(7) PSD3). The RTS will bring further harmonisation to an area that has been subject to significant divergence across Member States.

06 / OPEN BANKING 2.0: A FUNDAMENTALLY RESHAPED FRAMEWORK

PSR brings about a comprehensive overhaul of the open banking framework that was originally introduced by PSD2. For FinTechs operating as PISPs or AISPs, the changes are substantial and, in many respects, positive.

6.1 Dedicated Interfaces as the Norm

The PSR does not create the dedicated interface concept from scratch. The SCA RTS already require ASPSPs to maintain an access interface and set out detailed requirements for technical documentation, testing facilities, performance monitoring and quarterly publication of statistics. The important change is that the PSR makes the dedicated interface the default access route for AISPs and PISPs (Article 35 PSR), rather than one option alongside the customer-facing interface. ASPSPs may avoid the requirement only where a competent authority grants a derogation under Article 39 of PSR. This turns what was largely an RTS-based interface framework into a more prescriptive legislative obligation, with dedicated APIs becoming the norm rather than an implementation choice.

6.2 Data Parity and Prohibited Obstacles

PSR strengthens the data parity principle. The SCA RTS already require a dedicated interface to offer the same level of availability and performance, including support, as the ASPSP's own customer-facing online channels. The PSR carries that principle into primary legislation and expands it by requiring parity not only in performance, but also in the account and transaction information made available to AISPs and the initiation and execution information made available to PISPs (Article 37(2) and 37(3) PSR).

Additionally, Article 44(1) of PSR goes further by setting out a detailed list of twelve minimum specific prohibited obstacles that ASPSPs must not create. These obstacles include, for example, preventing the use of personalised security credentials by PISPs or AISPs, requiring manual entry of identifiers, imposing additional registrations or SCA steps beyond what is required for direct access, restricting payments to beneficiary lists and requiring dual SCA in payment initiation journeys. This granular approach is a significant improvement on the more general anti-obstacle provisions under PSD2 and the associated EBA guidelines.

6.3 The Consent Dashboard

A notable open banking innovation is the requirement for ASPSPs to provide a "dashboard" integrated into their user interface, enabling payment service users to monitor and manage the consents they have given to AISPs and PISPs (Article 43(1) PSR). The dashboard must display the identity of each third-party provider, the scope of data access, frequency of access and the duration of consent (Article 43(2) PSR). Users can withdraw or modify permissions directly through the dashboard (Article 43(2)(b) PSR). While this enhances consumer control, it also creates a mechanism by which users may more readily revoke access, which AISPs and PISPs will need to factor into their business planning.

6.4 Competent Authority Enforcement

PSR places a clear obligation on competent authorities to proactively enforce the open banking framework (Article 48 PSR), including by holding joint meetings with ASPSPs and third-party providers (Article 48(6) PSR), ensuring that prohibited obstacles are immediately removed (Article 48(1) PSR), and imposing sanctions where necessary. The EBA is tasked with coordinating monitoring activity across Member States (Article 48(7) PSR), which should help address the enforcement inconsistencies that plagued PSD2's open banking provisions.

07 / FRAUD PREVENTION: A NEW LAYER OF OBLIGATIONS

PSR introduces an extensive new suite of fraud prevention provisions that will impose significant obligations on payment institutions and FinTechs.

7.1 Transaction Monitoring

Similarly to PSD2, Article 83(1) of PSR requires all PSPs to have transaction monitoring mechanisms in place to support the application of SCA, determine SCA exemptions and detect and prevent potentially fraudulent transactions. Critically, under PSR the payer's PSP must carry out monitoring prior to the execution of a payment transaction, and the payee's PSP must carry out monitoring before making funds available to the payee (Article 83(1a) PSR). A failure to carry out such monitoring creates direct liability, as the PSP concerned must refund the payer the full amount of the transaction, save where the payer has acted fraudulently (Article 83(1a) PSR).

7.2 Mandatory Information Sharing

Article 83a(1) of PSR requires PSPs to participate in information sharing arrangements with other PSPs, exchanging data to the extent necessary for fraud detection. Limited categories of data may be shared, robust safeguards are required, including pseudonymisation, and there is a prohibition on retaining shared data beyond five years (Articles 83a(1) to (3) PSR). Importantly, PSPs are prohibited from taking adverse decisions, such as terminating a customer relationship, solely based on information received through these arrangements without conducting an independent assessment (Article 83a(5) PSR).

7.3 Impersonation Fraud Liability

Article 59 of PSR introduces a new liability regime for impersonation fraud, where a consumer is manipulated by a third party pretending to be the consumer's PSP using the PSP's own communication channels (e.g. spoofed phone numbers or email addresses). In such cases, the PSP must refund the consumer the full amount of the fraudulent transaction, provided the consumer notifies the PSP without undue delay and files a police report (Article 59(1) PSR). The PSP may refuse the refund only where it can demonstrate fraud or gross negligence by the consumer (Article 59(2)(b) PSR), with the burden of proof resting on the PSP (Article 59(4) PSR). This is a significant new exposure for payment institutions that will require investment in anti-spoofing technologies and robust communication channel security.

7.4 Payee Verification

Article 50 of PSR extends the "confirmation of payee" service to all credit transfers, not only SEPA transactions. This service requires PSPs to verify whether the name and unique identifier of the payee match before the execution of a transfer. Article 57 imposes liability on the payer's PSP where a failure to provide this verification service correctly results in a defectively executed payment.

08 / SCA: EVOLUTION, NOT REVOLUTION

PSR retains the core PSD2 framework for SCA but introduces several notable refinements and, critically, absorbs into the primary legislation much of the detail that currently sits in the SCA RTS. The requirement for SCA remains applicable when the payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel that may imply a risk of payment fraud (Article 85(1) PSR).

8.1 Changes to the Core SCA Framework

Key changes to the core SCA framework under PSR include:

- **Allowing SCA to be performed using two elements from the "inherence" category alone (e.g. two biometric factors), provided the PSP demonstrates to the competent authority that the elements are independent and the procedure ensures a high level of security (Article 85(12)).**
- **Clarification that merchant-initiated transactions are not subject to SCA, provided SCA is applied at the set-up of the initial mandate.**
- **Confirmation that mail order and telephone order transactions are not subject to SCA, provided security requirements and checks are carried out by the payer's PSP allowing a form of authentication.**
- **Specific SCA requirements for mobile application activation, including a mandatory four-hour delay period (adjustable by the user) before a remotely activated mobile application takes effect (Article 51(4b)), and SCA for the creation or replacement of tokenised payment instruments via a remote channel (Article 85(1)(d)).**

8.2 Interaction with the SCA RTS

The SCA RTS currently set out the detailed exemptions from SCA, including for:

- contactless payments at point of sale (Article 11 – individual transactions up to €50, cumulative cap of €150)
- low-value remote transactions (Article 16 – up to €30, cumulative cap of €100)
- transactions at unattended terminals for transport fares and parking fees (Article 12)
- trusted beneficiaries (Article 13)
- recurring transactions (Article 14)
- credit transfers between accounts of the same person (Article 15)
- secure corporate payment processes (Article 17)
- transaction risk analysis (Article 18 – based on fraud rate thresholds and real-time risk scoring)

The SCA RTS also specify the general transaction monitoring requirements (Article 2), the authentication code requirements (Article 4), dynamic linking requirements (Article 5) and the rules on confidentiality and integrity of personalised security credentials (Articles 22 to 24).

The EBA is mandated under Article 89(1) of PSR to develop new RTS that will replace the existing SCA RTS. The new RTS must specify:

- the requirements of SCA
- the exemptions from SCA, based on the criteria in Article 85(11), which now include whether or not the payer is a consumer, in addition to the existing criteria
- the security measures for protecting personalised security credentials
- requirements applicable to outsourcing agreements for SCA
- requirements for common and secure open standards of communication for open banking (including for the use of dedicated interfaces)
- technical requirements for transaction monitoring mechanisms

In relation to the exemption from SCA for payment transactions, the new SCA RTS must also specify, based on transaction risk analysis, the conditions for a remote electronic payment transaction to be considered low-risk, methodologies and models for transaction risk analysis, fraud rate calculation criteria and reporting and audit requirements (Article 89(1) PSR).

FinTechs and payment institutions currently relying on the existing SCA exemptions should note that while the broad categories of exemption are expected to be preserved, the specific thresholds, conditions and fraud rate requirements will be recalibrated in the new SCA RTS. In particular, PSR's explicit direction that the EBA must consider whether the payer is a consumer when designing exemptions (Article 85(11)(ca)) may lead to differentiated exemption regimes for consumer and non-consumer transactions, a significant change from the current one-size-fits-all approach in the existing SCA RTS.

8.3 AISP-Specific SCA Rules

Article 86(3) of PSR introduces a notable relaxation for account information services. The ASPSP must only apply SCA for the first access to payment account data by a given AISP, and not for subsequent accesses, unless the ASPSP has reasonable grounds to suspect fraud. AISPs must separately apply SCA when the payment service user accesses account information at least 180 days after SCA was last applied and may use their own or the ASPSP's SCA for this purpose (Article 86(4) PSR). Under the existing SCA RTS, the ASPSP bears the obligation to re-apply SCA after 180 days of AISP access (Article 10a, as amended). The key change under PSR is, therefore, not the period itself, but the shift in responsibility, as the ASPSP is relieved of periodic re-authentication entirely (needing only to authenticate on first access), while the 180-day re-authentication obligation is placed squarely on the AISP (Article 86(4) PSR).

8.4 Accessibility

Of particular importance for FinTechs is the new accessibility requirement in Article 88 of PSR. PSPs must ensure that all customers, including persons with disabilities, older persons, those with low digital skills and those without access to digital channels, have at least one means of performing SCA free of charge (Article 88(1) PSR). PSPs must not make SCA dependent on the exclusive use of a smartphone or other smart device unless the user has agreed to mobile-only services (Article 88(2) PSR). PSPs must develop more than one means for performing SCA and ensure users are adequately informed of the options available to them.

9 / OEMS AND MOBILE DEVICE ACCESS: THE FRAND OBLIGATION

Article 88a of PSR introduces what is arguably one of the most consequential provisions for the technology sector. OEMs of mobile devices and electronic communications service providers must allow PSPs and their technical service providers effective interoperability with, and access for the purposes of interoperability to, hardware and software features that are necessary for securely processing and executing payment transactions (Article 88a(1) PSR). This encompasses features such as NFC technology, secure elements and payment terminal kernels.

This access must be provided on FRAND terms (Article 88a(1) PSR). OEMs may take strictly necessary and proportionate measures to protect the integrity of their hardware and software (Article 88a(2) PSR) but must publish general conditions of access (Article 88a(3) PSR). The European Commission has exclusive supervisory and enforcement powers where these obligations apply to very large online platforms and search engines (Article 89a PSR).

The introduction of Article 88a directly addresses the competitive concerns raised by FinTechs and PSPs regarding access to the NFC antenna and secure element on mobile devices, features that have historically been controlled by a small number of OEMs.

It should open up the mobile payments market to greater competition, though the practical implementation of FRAND terms will likely be a source of ongoing negotiation and, potentially, dispute.

10 / ACCESS TO PAYMENT SYSTEMS AND SCHEMES

PSR strengthens the rules on access by payment institutions to payment systems and, in a new provision, applies the rules to payment schemes. Payment system operators must maintain objective, non-discriminatory, transparent and proportionate access rules, and may only refuse participation where the applicant poses genuine risks to the system (Article 31(1) PSR). Article 31(5a) of PSR extends similar principles to payment scheme operators, requiring them to publish admission rules and risk assessment criteria and to carry out risk assessments of applicants.

For FinTechs, the reinforced access provisions, combined with the enhanced "de-risking" protections in Article 32 of PSR (requiring credit institutions to provide payment account access to payment institutions on an objective, non-discriminatory and proportionate basis), should help address the significant practical barriers that payment institutions have faced in accessing payment infrastructure and maintaining banking relationships.

11 / CROSS-SECTORAL COOPERATION AND THE WIDER ECOSYSTEM

PSR reaches beyond the traditional payments perimeter to impose obligations on electronic communications service providers and providers of very large online platforms and search engines in the fight against payment fraud.

Telecommunications providers and very large online platforms and search engines must establish dedicated communication channels with PSPs for fraud data exchange (Article 59a(2) PSR), implement educational measures for their users regarding online scams (Article 59a(3) PSR). Telecomunications providers must also take appropriate organisational and technical measures to detect and prevent the use of their services for impersonation fraud, including manipulation of email and calling line identification (Article 59a(5) PSR).

Very large online platforms and search engines must request from advertisers of regulated financial services information attesting to authorisation or registration and must refuse to carry such advertising where the information is not provided (Article 59b(1) to (3) PSR). This aims to combat the fraudulent promotion of financial services that often underlies authorised push payment fraud.

12 / ENFORCEMENT AND SANCTIONS

PSR introduces a significantly more detailed enforcement framework (Articles 89a to 103 PSR), including mandatory administrative sanctions for specific infringements such as breaches of open banking rules, SCA obligations and refund timelines (Article 97(1) PSR). Maximum fines for legal persons are set at 10% of total annual net turnover (Article 97(2)(a)(i) PSR). For natural persons, the maximum fine is €3 million (Article 97(2)(a)(ii) PSR). New provisions on the publication of enforcement decisions and whistleblowing protections round out the regime (Article 101 PSR). Under the Central Bank of Ireland's administrative sanctions regime, a maximum fine of up to 10% of turnover is already provided for in the case of legal persons. However in the case of natural persons, the maximum fine is currently €1 million.

13 / CRYPTO-ASSET INTEGRATION

In a targeted but important amendment, Article 110b of PSR modifies the Markets in Crypto Assets Regulation (Regulation (EU) 2023/1114) to allow payment institutions authorised under PSD3 to provide certain crypto-asset services in relation to e-money tokens for payment purposes. This is subject to a 40-working-day advance notification to the competent authority and operates on the basis of a deemed equivalence between the specified crypto-asset services and corresponding payment services. For FinTechs at the intersection of payments and digital assets, this creates a streamlined route to market.

14 / PREPARING FOR THE TRANSITION

The timeline for compliance is tight. PSD3 must be transposed by Member States within 21 months of its entry into force (Article 49 PSD3) and PSR will apply from the same date (Article 112 PSR). The payee verification (confirmation of payee) provisions carry a slightly longer lead-in of 27 months (Article 112 PSR).

For payment institutions, EMIs, FinTechs and OEMs, the key preparatory steps include:

- reviewing authorisation status and, for EMIs, planning for transition to the unified PI regime
- assessing capital and own funds positions against the new thresholds and methodologies
- reviewing safeguarding arrangements and preparing winding-up plans
- upgrading transaction monitoring systems and establishing or joining information sharing arrangements
- ensuring SCA accessibility compliance
- for OEMs only, establishing FRAND access terms for payment-relevant hardware and software features

The new framework is ambitious in scope and represents a genuine step-change in the regulation of the EU payments market. Firms that begin their gap analysis now will be best placed to navigate the transition successfully.

15 / HOW CAN ALG HELP?

The introduction of PSD3 and PSR represents a significant and wide-ranging transformation of the EU payments framework, with important operational, prudential and conduct implications for payment institutions, EMIs, PISPs, AISPs, OEMs and certain technology providers. ALG's dedicated FinTech Team is well placed to support clients across all stages of implementation.

ALG can assist firms in conducting a comprehensive gap analysis of their existing business models, authorisation status and operational frameworks against the requirements of PSD3 and PSR, identifying the key areas where changes to governance, policies, systems and controls will be required. In particular, we can support EMIs in navigating the transition to the new unified payment institution regime, including advising on authorisation strategy, capital and own funds requirements, and engagement with the Central Bank of Ireland.

Our team can provide practical guidance on the enhanced safeguarding and prudential requirements, including the design of compliant safeguarding arrangements and the preparation of winding-up plans. We can also advise on the implementation of updated SCA requirements, strengthened fraud prevention obligations, including transaction monitoring frameworks, participation in information-sharing arrangements and the management of new liability exposures.

In relation to the open banking framework, ALG can assist ASPSPs, PISPs and AISPs in adapting to the new requirements, including API compliance, removal of prohibited obstacles, implementation of consent dashboards and alignment with data parity obligations.

More broadly, ALG supports clients in engaging with regulatory developments at both EU and national level, including tracking Irish transposition measures, interpreting Level 2 and 3 measures as they emerge and preparing for supervisory scrutiny. We work closely with clients to deliver practical, tailored solutions to support efficient and timely implementation of the new regime.

16 / YOUR ALG FINTECH TEAM

Eimear O'Brien
Partner
+353 1 649 2460
eobrien@algoodbody.com

Louise Hogan
Partner
+353 1 649 2961
lahogan@algoodbody.com

Eoin O Connor
Partner
+353 1 649 2367
eoconnor@algoodbody.com

Patrick Brandt
Partner
+353 1 649 2337
pbrandt@algoodbody.com

Sarah Lee
Senior Knowledge Lawyer
+353 1 649 2105
salee@algoodbody.com

A&L Goodbody

DUBLIN

A&L Goodbody LLP
25 North Wall Quay
Dublin 1
D01 H104
Ireland

BELFAST

A&L Goodbody Northern Ireland LLP
42 - 46 Fountain Street
Belfast BT1 5EF
Northern Ireland

LONDON

A&L Goodbody
Augustine House
Austin Friars
London EC2N 2HA
United Kingdom

NEW YORK

A&L Goodbody LLP
The Chrysler Building
405 Lexington Avenue
New York, NY 10174
USA

SAN FRANCISCO

A&L Goodbody LLP
580 California Street
Suite 1200
PMB #86803
San Francisco, CA 94104
USA