MEXC

After MiCA Week One

EU Onboarding, Payment Rails and the Finetix – OuiTrust/Heuro – Ocean Wave – Legend Trading Relay

Master Compliance Intelligence Report

MiCA/MiFID-II Perimeter Radar Case File — Radar Status: Black / Active EU Onboarding Watch

Field	Detail
Document class	Compliance intelligence memorandum (publication-ready basis)
Prepared by	FinTelegram News — Cyberfinance Intelligence & Compliance Desk
Intended audience	EU regulators and supervisors (ESMA, EBA, NCAs); compliance functions at EMIs, PSPs, banks, CASPs and card acquirers; law-enforcement and institutional counterparties
Date of issue	5 July 2026
Version	1.1 — subject to update upon right-of-reply responses and new evidence

Field	Detail
Evidence standard	Four-tier framework: Established Fact / Strong Indicator / Reasonable Hypothesis / Open Question (see Section 1.4)
Legal note	This report analyses regulatory and compliance risk only. It does not allege that any person or entity has committed a criminal offence.

Content

1. Executive Summary

1.1 Purpose and headline finding

On 1 July 2026, the transitional period under the **Markets in Crypto-Assets Regulation (MiCA**, Regulation (EU) 2023/1114) ended across the European Economic Area. From that date, the provision of crypto-asset services to EU clients requires authorisation as a crypto-asset service provider (CASP) under MiCA Article 59, and the European Securities and Markets Authority (ESMA) has stated publicly that unauthorised CASPs must immediately stop onboarding new EU clients, refrain from opening new client relationships or accounts, cease marketing and solicitation, and restrict remaining activity to an orderly wind-down (ESMA, Public Statement ESMA75-113276571-1710, 23 June 2026).

Against that benchmark, this report documents and analyses the post-MiCA EU-facing behaviour of the offshore crypto exchange operating under the MEXC brand (mexc.com). The headline finding is stark and, in FinTelegram's assessment, of immediate supervisory relevance: **on MiCA Day One, 1 July 2026, MEXC accepted and fully verified a new EU retail user, enabled fiat and crypto deposit functionality, and disclosed no MiCA authorisation, no MiCA-authorised EU legal entity and no wind-down or restriction notice anywhere in the tested user journey** (FinTelegram, MiCA/MiFID-II Perimeter Radar: MEXC Still Onboards EU Users On MiCA Day One, 1 July 2026). No MEXC entity appears in the ESMA MiCA register reviewed by FinTelegram, and no MEXC entity has publicly disclosed a CASP authorisation.

This behaviour is documented as tested platform conduct — screenshots and verification e-mails are on file — and not as speculation. It stands in direct tension with ESMA's Day One expectations and with MEXC's own published content, which acknowledges that firms without a MiCA licence can no longer legally serve EU users after 1 July 2026 (FinTelegram, 1 July 2026, citing MEXC's news portal).

1.2 The payment relay behind EU fiat access

A follow-up forensic test of MEXC's fiat deposit and buy-crypto flows, published by FinTelegram on 2 July 2026, indicates that MEXC has not merely left its platform open to EU users. The tested flows routed a KYC-verified EU user through a **multi-layer chain of third-party service providers** while keeping the MEXC trading and deposit experience functionally intact (FinTelegram, MEXC Update: The Finetix–OuiTrust–Ocean Wave–Legend Trading Payment Relay Exposed, 2 July 2026). The observed architecture can be summarised as: EU user → MEXC onboarding → MEXC fiat deposit / buy-crypto flow → third-party consent or account creation → Finetix / OuiTrust–Heuro / Ocean Wave / Legend Trading layers → EUR bank transfer or card payment → crypto or fiat crediting inside the MEXC environment.

Four third-party layers were documented in the tested flows:

- **Finetix Limited S.R.L.** (Bucharest, Romania, reg. no. 51736231) — self-described on finetix.net as a Romania-based crypto exchange offering fiat payment gateway services across European jurisdictions; its Terms of Use state that Finetix acts as principal in digital-asset transactions and relies on partnered payment institutions. A card-payment verification screenshot in the MEXC flow displayed the descriptor **Finetix*mexc.com**.

- **Harmoniie SAS, since December 2025 Heuro SAS, doing business as OuiTrust** — a French electronic money institution (EMI) authorised by the ACPR under licence no. 17478, BIC HRSAFR22. MEXC's EUR bank-transfer flow presented a consent screen referencing MEXC and Harmoniie SAS dba OuiTrust, with links to OuiTrust and Finetix legal materials, and then generated a concrete EUR 100 payment order to a **French IBAN at Heuro** for the EU test user.
- **Ocean Wave Fintech Pty Ltd** (Australia, ABN 59 638 473 211) — during the deposit process, a Service Provider Change Confirmation screen stated that the service would henceforth be provided from Australia, and account-creation e-mails were automatically triggered. Public ABN records show that this entity previously traded as **MEXC Australia Pty Ltd** and **MXC Tech Pty Ltd** (Australian Business Register).
- **Legend Trading / Legend Financial Ireland Limited** — a MiCA-authorised CASP (Central Bank of Ireland, authorisation announced 13 October 2025). A separate MEXC buy-crypto-by-bank-transfer flow triggered an account application with Legend, requiring acceptance of Legend's terms and generating MEXC-via-Legend onboarding e-mails.

FinTelegram does not allege that MEXC, Finetix, Heuro/OuiTrust, Ocean Wave and Legend Trading are under common ownership, and this report draws no such conclusion. What the documented flows do establish is that, days after the MiCA transition deadline, an EU retail user could still move euros into the MEXC environment through a relay of EU-regulated and third-country service providers — a pattern that is difficult to reconcile with an orderly wind-down posture and that raises perimeter, outsourcing, conduct and AML/CFT questions for every institution in the chain.

1.3 Context: a documented regulatory history

The MiCA Day One findings do not arise in a vacuum. MEXC-branded operations have accumulated a substantial adverse regulatory record: the UK FCA lists MEXC Global Ltd on its Warning List as an unauthorised firm; Australia's MoneySmart (ASIC) carries an investor alert for MEXC Global (mexc.com); the Belgian FSMA ordered Mexc Global LTD in July 2024 to cease custodian wallet services in Belgium and to cease distributing to Belgian retail clients financial products whose return depends on virtual money; and on 26 May 2026 the Seychelles FSA identified MX Global Ltd (IBC 238047) as the entity operating the MEXC platform without the licence required under the Seychelles VASP Act, 2024, after the previously associated company, MEXC Global LTD (IBC 218833), had been struck off and dissolved. Additional warnings have been reported from BaFin (Germany), the Austrian FMA, the Netherlands AFM, Hong Kong's SFC and the Securities Commission Malaysia.

On the payment-rail side, the Bank of Lithuania revoked the EMI licence of **Paytend Europe UAB** in early March 2026 for serious and systematic AML/CFT and internal-control failures, including the provision of incorrect information about a business relationship with an unnamed high-risk customer. FinTelegram had publicly warned Paytend in February 2026 that its rails were facilitating MEXC-related euro deposits via Finetix. Following the revocation, FinTelegram's July 2026 testing indicates that the MEXC euro rail has been re-engineered around the Finetix / Heuro–OuiTrust / Ocean Wave / Legend architecture described above.

1.4 Evidence standards used in this report

Every material statement in this report is assigned, explicitly or by context, to one of four evidence tiers. Readers, supervisors and counsel should treat the tiers as strict boundaries on the weight each statement can bear:

- **ESTABLISHED FACT (documented and cross-confirmed)** — supported by primary sources (regulatory statements, official registers, statutory filings) or by multiple independent, consistent sources.
- **STRONG TECHNICAL / DOCUMENTARY INDICATOR** — supported by direct documentary or technical evidence (screenshots on file, platform e-mails, website terms, traffic or descriptor analysis), typically from FinTelegram's own testing, but not yet confirmed by the entities concerned or by a regulator.
- **REASONABLE HYPOTHESIS** — an explicitly labelled, testable working assumption consistent with the evidence, which further documents, whistleblower material or regulatory disclosure could confirm or refute.
- **OPEN QUESTION / INFORMATION GAP** — a point on which the available evidence permits no responsible conclusion.

FinTelegram articles are treated throughout as investigative secondary sources; statements by regulators, official registers and statutory filings are treated as primary sources. Ownership and beneficial-ownership language is kept strictly conditional. Nothing in this report states or implies that any named person or entity has committed fraud, money laundering or any other criminal offence; the analysis is confined to regulatory and compliance risk. All named entities are invited to respond under the right-of-reply framework in Section 8, and their statements will be incorporated into updated versions of this report.

2. Regulatory Framework and MiCA Day One Obligations

2.1 MiCA and the end of the transitional period

MiCA established the EU's first harmonised authorisation regime for crypto-asset services. Article 59 prohibits the provision of crypto-asset services in the Union without CASP authorisation, and Article 143(3) allowed providers that were operating lawfully under national regimes before 30 December 2024 to continue during a transitional period while seeking authorisation. That transitional window closed definitively on **1 July 2026**; several Member States applied shorter periods that expired earlier (for example, the Netherlands, Finland, Latvia, Hungary and Slovenia at six months, and Sweden at nine months). From 1 July 2026, legacy national VASP registrations, pending applications and application reference numbers confer no right to serve EU clients: only a granted MiCA authorisation does. (**Established fact** — MiCA; ESMA statements of 4 December 2025, 17 April 2026 and 23 June 2026; national regulator communications.)

The relevant MiCA crypto-asset services include custody and administration of crypto-assets, operation of a trading platform, exchange of crypto-assets for funds or for other crypto-assets, execution of orders, placing, transfer services, and related advice or portfolio management. A centralised exchange offering EU retail users account opening, spot trading, custody-style wallets, fiat on-ramping and crypto transfers engages several of these services simultaneously.

2.2 ESMA's Day One expectations for unauthorised CASPs

In its Public Statement of 23 June 2026 (ESMA75-113276571-1710), ESMA set out the operative standard against which post-deadline conduct must be measured. Unauthorised CASPs must immediately stop onboarding new EU clients, refrain from opening new client relationships or accounts, and cease marketing and solicitation; they must limit services to actions necessary to sell or transfer crypto-assets, reallocate assets or close positions; and custody may continue only for the period strictly necessary to complete an orderly exit. ESMA further reminds CASPs established outside the EU that they cannot provide MiCA services to EU clients or solicit EU clients — including in a business-to-business context — except under the narrow reverse-solicitation regime, and that MiCA prohibits CASPs from outsourcing or delegating certain services, notably custody, to entities that are not authorised CASPs. Clients of unauthorised providers do not benefit from MiCA safeguards, including client-asset protections, and are invited to verify their provider's status in the ESMA register. (**Established fact** — ESMA, 23 June 2026; mirrored by the AMF and other NCAs.)

ESMA also announced that it and national competent authorities are directly engaged with the entities concerned, will monitor whether significant unauthorised cross-border CASPs wind down without delay, and will work with the EBA and AMLA, with NCAs able to take coordinated action after the transitional period. Wind-downs must be conducted in full compliance with AML/CFT obligations, including customer due diligence, transaction monitoring, sanctions screening, suspicious-transaction reporting and transfer-traceability requirements. Where clients are migrated to an authorised CASP, the receiving CASP must conduct its own onboarding and AML/CFT checks — clients cannot simply be shifted between group companies or platforms.

Market context underlines how selective the authorised perimeter is: industry data cited in trade press around the deadline suggested that only roughly 210 of more than 1,200 entities holding pre-MiCA national registrations had converted to CASP status — a conversion rate below 18% — with around ten EU jurisdictions yet to issue a single CASP licence. (**Strong indicator** — Kaiko data as reported by The Full FX, 25 June 2026; not independently verified by FinTelegram.)

2.3 The MiFID II / CFD perimeter for crypto derivatives

MiCA is not the only perimeter engaged by MEXC's product set. MEXC prominently offers futures and other leveraged derivatives-related products, and its User Agreement expressly refers to risks associated with transactions in digital assets and their derivatives (**strong indicator** — MEXC User Agreement as reviewed by FinTelegram, 1–2 July 2026). Crypto perpetual futures and similar leveraged contracts offered to EU retail clients may constitute financial instruments under MiFID II, triggering investment-services licensing requirements and the product-intervention framework applicable to CFDs and similar leveraged retail products, including leverage caps, margin-close-out rules, negative-balance protection and marketing restrictions applied by NCAs. For EU retail users, MEXC's offering therefore presents a **dual perimeter problem**: MiCA for crypto-asset services such as trading, custody, exchange and transfer; and MiFID II / product-intervention rules for futures and derivatives linked to crypto-assets. The Belgian FSMA's 2024 order — which targeted, in addition to custody wallets, the distribution to retail clients of financial products whose return depends directly or indirectly on virtual money — anticipated exactly this dual exposure. (**Established fact** as to the FSMA order; **reasonable hypothesis**, to be assessed instrument-by-instrument, as to the MiFID II characterisation of specific MEXC products.)

2.4 Why payment rails are the enforcement frontier

The practical effectiveness of the MiCA perimeter depends on the fiat ramp. If an unauthorised offshore exchange can continue to receive euros from EU consumers through European banks, EMIs, payment institutions and card acquirers, the licensing regime risks becoming only partially effective. Regulated payment intermediaries are therefore expected — under their own AML/CFT, safeguarding and conduct frameworks — to know whether the crypto counterparties behind their merchant flows are authorised under MiCA, operating under a valid transitional arrangement, or outside the authorised perimeter, including where flows are routed through intermediaries, merchant-of-record constructions or offshore entities that obscure the real crypto counterparty. This report examines MEXC's EU rails through exactly that lens.

3. MEXC Operator Profile and Regulatory History

3.1 Corporate footprint and known legal entities

The MEXC brand (founded 2018, formerly MXC Exchange) is operated through a shifting set of offshore and satellite entities. No consolidated group structure, audited group accounts or beneficial-ownership disclosure for the platform as a whole is publicly available, and MEXC's own sites provide inconsistent compliance disclosures (**strong indicator** — FinTelegram compliance updates, 2024–2026). The entities most relevant to EU supervision are set out below.

Entity	Jurisdiction	Status and relevance
MEXC Global LTD (IBC 218833)	Seychelles	Historical operator entity named on regulator warnings (FCA, FSMA, ASIC/MoneySmart). Struck off the Seychelles register on 17 August 2023 and automatically dissolved on 18 December 2024; never licensed under the Seychelles VASP Act. (Established fact — Seychelles FSA, 26 May 2026.)
MX Global Ltd (IBC 238047)	Seychelles	Identified by the Seychelles FSA on 26 May 2026 as the entity operating mexc.com without the required VASP licence, in breach of s.5 of the VASP Act, 2024 and s.5(2)(g)(ii) of the IBC Act, 2016; enforcement measures initiated, including referral to the competent authority. (Established fact — Seychelles FSA.)
MEXC Estonia OÜ	Estonia	Historical EU fiat-processing arm reported by FinTelegram (May 2024) as routing bank-transfer flows via Paytend Europe UAB; recorded UBO Yichen Peng per Estonian registry data cited by FinTelegram. (Strong indicator — FinTelegram / Teatmik.)
Oceanblue Fintech UAB (reg. 306111081), formerly MEXC Lithuania UAB	Lithuania	Reported by FinTelegram (October 2025) as operator of MEXC fiat services under a legacy Lithuanian VASP registration, with payment accounts provided by Paytend Europe UAB; no public evidence of a MiCA authorisation. The rebrand away from the MEXC name is itself a compliance signal. (Strong indicator — FinTelegram; Lithuanian registry.)

Entity	Jurisdiction	Status and relevance
Ocean Wave Fintech Pty Ltd (ABN 59 638 473 211)	Australia	Australian private company whose ABN history shows prior names MXC Tech Pty Ltd, MEXC Australia Pty Ltd and Ocean Waive Fintech Pty Ltd; appeared in MEXC's July 2026 EU deposit flow as incoming service provider. (Established fact as to the name history — Australian Business Register; see Section 5.4.)

The pattern visible in this table — dissolution of the publicly named operator, emergence of a successor IBC, and renaming of satellite entities away from the MEXC label (MEXC Lithuania → Oceanblue; MEXC Australia → Ocean Wave) — is, at minimum, a **strong indicator of deliberate corporate opacity** in the sense used in AML/CFT risk assessment. Whether it reflects a coordinated strategy to detach EU and other customer relationships from identifiable MEXC entities is a **reasonable hypothesis** that only contracts, corporate records and insider evidence can confirm (see Sections 7 and 9).

3.2 Regulatory warnings and enforcement record

3.2.1 Seychelles FSA (primary)

The Seychelles Financial Services Authority publicly flagged the platform's non-compliance in press releases of 14 February 2025 (failure of MEXC Global LTD to submit a licence application) and 30 May 2025 (confirmation that MEXC Global LTD had been dissolved and had never held any authorisation for virtual-asset activities). On 26 May 2026, following supervisory and investigative work conducted in collaboration with local and international regulatory partners, the FSA announced that it had positively identified MX Global Ltd as the operator of the MEXC platform, determined that it had been carrying on virtual-asset services in or from Seychelles without authorisation since 1 January 2025, warned investors and counterparties to exercise extreme caution, and stated that it cannot investigate complaints or facilitate recovery of funds because the entity is unsupervised. (**Established fact.**)

3.2.2 United Kingdom — FCA (primary)

MEXC Global Ltd (mexc.com) appears on the FCA Warning List as a firm that may be promoting financial services or products without authorisation. The FCA advises consumers to avoid dealing with the firm and notes that users have no access to the Financial Ombudsman Service or the FSCS. (**Established fact** — FCA Warning List.) Subsequent reporting indicates that MEXC has moved the UK to a fully prohibited jurisdiction in its User Agreement, consistent with the FCA financial-promotions regime in force since October 2023.

3.2.3 Australia — ASIC / MoneySmart (primary)

MEXC Global (www.mexc.com) is carried on the MoneySmart Investor Alert List maintained by ASIC, which flags entities that could be operating without an appropriate Australian licence. MEXC holds no

ASIC licence and no publicly identified AUSTRAC digital-currency-exchange registration for the platform. (**Established fact** as to the alert listing; the AUSTRAC point is a **strong indicator** pending registry confirmation.) The relevance of this alert is amplified by the appearance of an Australian entity — Ocean Wave Fintech Pty Ltd — inside MEXC's EU deposit flow (Section 5.4).

3.2.4 Belgium — FSMA order (primary)

By order published in July 2024, the FSMA required Mexc Global LTD to cease providing all custodian wallet services in Belgium and to cease all distribution to Belgian retail clients of financial products whose return depends, directly or indirectly, on virtual money. The FSMA stated that, by offering such services in Belgium from the Seychelles — a non-EEA jurisdiction — the firm was violating the Belgian prohibition on third-country providers, breach of which carries criminal sanctions under Article 136 of the Belgian AML Law, and directed that Belgian clients' wallets be transferred to a duly authorised EEA custodian. (**Established fact** — FSMA, Mexc Global LTD order, July 2024.) The order is doubly significant: it evidences both the custody/exchange perimeter problem now generalised by MiCA and the derivatives/product perimeter problem discussed in Section 2.3.

3.2.5 Further reported warnings

FinTelegram's October 2025 compliance update, citing the respective regulators, additionally lists a BaFin consumer warning and investigation notice (Germany), an Austrian FMA warning that MEXC is not authorised for licensable banking or financial activities in Austria, and inclusion on the Hong Kong SFC's list of suspicious virtual-asset trading platforms; the Securities Commission Malaysia placed MEXC Global on its Investor Alert List for operating a digital-asset exchange without registration; and a summary of the Seychelles action by compliance publisher Comsure records that the Netherlands AFM has publicly warned that MEXC operates without MiCA authorisation. (**Strong indicators** — secondary reporting of primary warnings; each entry should be verified against the issuing regulator's register before being relied upon in supervisory action.)

3.3 Succinct risk profile

Taken together, the record supports the following compliance characterisation, phrased deliberately in risk terms rather than as accusation: **multiple offshore and satellite entities with a pattern of renaming and dissolution; no disclosed MiCA authorisation or MiCA-authorised EU operating entity; repeated public warnings and orders from at least seven supervisory authorities across three continents; identification by its home-jurisdiction regulator as an unlicensed operator; opaque ownership and inconsistent operator disclosure; and a derivatives-heavy retail product set engaging perimeters beyond MiCA.** For any EU-regulated financial institution, this profile places MEXC-related flows squarely in the highest customer/counterparty risk category under standard AML/CFT risk-rating methodologies, independently of any conclusion about the platform's intent.

4. EU Onboarding Test on MiCA Day One

4.1 Test design and status of the evidence

On 1 July 2026, FinTelegram conducted a live onboarding test of mexc.com from within the European Union, as an EU resident and EU national, and extended the test to the platform's fiat deposit flows in the days immediately following. The findings below are **tested platform behaviour, documented by screenshots and platform e-mails held on file by FinTelegram** — they are not inferences from terms of service or marketing material. They carry the evidentiary status of strong technical/documentary indicators: directly documented, reproducible in principle, but not yet confirmed or explained by MEXC, which is invited to respond under Section 8. Reporter-specific identifiers, full IBANs and personal data are withheld from publication on data-protection and security grounds.

4.2 What the test established

The registration path accepted the EU user without geo-blocking, residency-based refusal or any MiCA-related interstitial. Advanced KYC was completed: identity and address verification were submitted and **approved**, confirmed by MEXC verification e-mails. The newly verified account received a confirmation that its 24-hour withdrawal limit had been raised to **200 BTC** — a limit that, at prevailing prices, corresponds to an institutional-scale daily withdrawal capacity being granted to a brand-new retail account. The platform then presented functional deposit options to the user, including bank transfer, debit/credit card, P2P routes and third-party providers, alongside ordinary crypto deposit functionality.

Equally significant is what the tested journey did **not** contain. FinTelegram observed no prominent MiCA restriction, no wind-down notice, no statement that new EU business had ceased, no disclosure of a MiCA-authorised EU legal entity, and no EU regulatory-status notice on the onboarding path or in the received e-mails. MEXC's User Agreement, as reviewed, lists numerous prohibited jurisdictions — including the United States, United Kingdom, Canada, mainland China and Singapore — but does not name EU or EEA states as such, and MEXC's own support materials continued to describe EUR online bank-transfer deposits as available to verified KYC users from a list of supported countries including Austria, Belgium, France, Germany, Ireland, Italy, Lithuania, Luxembourg, Malta, Poland, Romania and Spain, with fiat deposit limits of up to EUR 20,000 per transaction and EUR 200,000 per day. (**Strong indicators** — FinTelegram, 1–2 July 2026, with screenshots on file; MEXC support pages and User Agreement as reviewed.)

4.3 Why this conflicts with ESMA's Day One expectations

Measured against the ESMA standard set out in Section 2.2, each element of the tested journey points the same way. Accepting a new EU registration is onboarding a new EU client. Approving advanced KYC and opening functional account capability is opening a new client relationship or account. Presenting deposit routes and granting a 200 BTC withdrawal limit is the opposite of limiting services to what is necessary to sell, transfer, reallocate or close positions. And the absence of any restriction or wind-down communication is difficult to reconcile with ESMA's requirement that providers

communicate clearly, promptly and repeatedly about their wind-down. In FinTelegram's assessment: **if a non-MiCA-authorised offshore exchange accepts a new EU customer, verifies EU identity and address, and enables deposits on 1 July 2026, this is not orderly wind-down; it is apparent continuation of EU-facing crypto services.** The characterisation apparent continuation is used advisedly: MEXC may assert a reverse-solicitation defence or point to arrangements not visible in the user journey, and any such explanation will be reported. The reverse-solicitation exemption is, however, narrow, applies only to services provided at the client's own exclusive initiative, and — per ESMA guidance — cannot be engineered through broadly accessible interfaces that actively serve EU users.

This is the reason FinTelegram classifies MEXC under its MiCA/MiFID-II Perimeter Radar as **Radar Status: Black — Active EU Onboarding Watch / Payment Rails Watch / MiFID-II Derivatives Watch**, the third Radar case after Hyperliquid (on-chain perpetuals perimeter) and Dream Finance / CoinsPaid / CryptoProcessing (restricted-activity payment processor). MEXC is analytically distinct from both: it presents as the offshore exchange that simply continues as before.

4.4 Reverse Solicitation: Why It Appears Weak Here

The reverse-solicitation argument appears **weak on the currently documented facts**. Under MiCA and ESMA's post-transition guidance, the exemption is narrow and applies only where a specific crypto-asset service is provided at the client's own exclusive initiative, without prior marketing, solicitation, targeting, or the maintenance of a generally accessible EU-facing onboarding path by the provider.MEXC_MiCA_Day_One-CR-v1.docx

That standard does not sit comfortably with the conduct documented in this file. FinTelegram's testing indicates that, after 1 July 2026, an EU resident could access the ordinary MEXC registration flow, complete KYC, open a fully functional account, receive confirmation of a 200 BTC withdrawal limit, and access fiat and crypto deposit functionality without any visible friction, MiCA restriction, or wind-down warning addressed to EU users. Such a flow looks less like a genuinely exceptional, client-initiated approach and more like the continued availability of a standardised service architecture to EU retail users.

The weakness of a reverse-solicitation theory is reinforced by the surrounding payment design. The documented EUR funding routes did not terminate at a simple "service unavailable in the EU" boundary; instead, they routed the user through layered third-party consent, onboarding, and payment steps involving Finetix, Heuro/OuiTrust, Ocean Wave Fintech, and Legend Trading while preserving the practical ability to move funds into the MEXC environment. If a platform keeps its EU-facing onboarding path open and supplements it with functioning fiat rails, that is difficult to reconcile with the notion that services are being provided only in isolated cases at the user's sole initiative.MEXC_MiCA_Day_One-CR-v1.docx

This does not mean that a reverse-solicitation defence is legally impossible. MEXC or any involved intermediary may argue that the user approached specific services independently, that the relevant transaction was executed by a separate regulated third party, or that the exchange itself did not actively target the EU user in the legally relevant sense. But on the facts currently documented, reverse solicitation appears at most a **possible defence theory**, not a persuasive explanation for the overall architecture observed after MiCA Day One.MEXC_MiCA_Day_One-CR-v1.docx

For supervisory purposes, the key question is therefore practical rather than theoretical: **does the totality of the onboarding, verification, deposit and payment-rail design amount to continued EU-facing service availability?** On the evidence currently described in this report, that question appears more likely to be answered yes than no.

5. MEXC EU-Facing Ecosystem and Payment Relay

5.1 Ecosystem Overview: Platform, Linked Entities and Relay Layers

The findings documented in this report are best understood not as a series of isolated bilateral relationships, but as an EU-facing service ecosystem surrounding the MEXC platform. The term **ecosystem** is used here descriptively. It does not imply common ownership, group control, coordinated misconduct or a single contractual chain between all entities shown. Rather, it captures the combination of platform operators, historically MEXC-linked entities, payment intermediaries, regulated financial institutions and third-country service-provider layers that appeared in public records or in FinTelegram's tested user journeys.

That distinction is important. A user interacting with mexc.com does not necessarily perceive the legal or regulatory boundaries between the different entities appearing behind registration, KYC, fiat funding, account creation, payment execution and crypto delivery. From a compliance perspective, however, those boundaries are decisive. The regulatory status of the exchange, the legal identity of the client-facing entity, the allocation of AML/CFT responsibilities, the handling of fiat and crypto value, and the status of each intermediary must be assessed separately.

FinTelegram's post-MiCA testing indicates that the practical EU-facing architecture cannot be reduced to a single MEXC operator. The observed environment comprises three broad layers:

1. **The EU user and regulatory perimeter** — a newly onboarded EU retail user interacting with the platform after 1 July 2026, against the background of MiCA, the MiFID II derivatives perimeter and ESMA's post-transition expectations.

2. **The MEXC platform and MEXC-linked operator or satellite entities** — including the central mexc.com trading environment, MX Global Ltd in Seychelles as the entity publicly identified by the Seychelles FSA as operating the platform without the required local VASP authorisation, and historical EU-facing entities such as Oceanblue Fintech UAB / MEXC Lithuania UAB.

3. **The EU-facing payment and onboarding relay** — including Finetix Limited S.R.L., Heuro/OuiTrust, Ocean Wave Fintech Pty Ltd and Legend Trading / Legend Financial Ireland Limited, each appearing in a different functional or regulatory capacity within tested or previously documented MEXC-related flows.

The following figure provides a high-level map of that architecture.

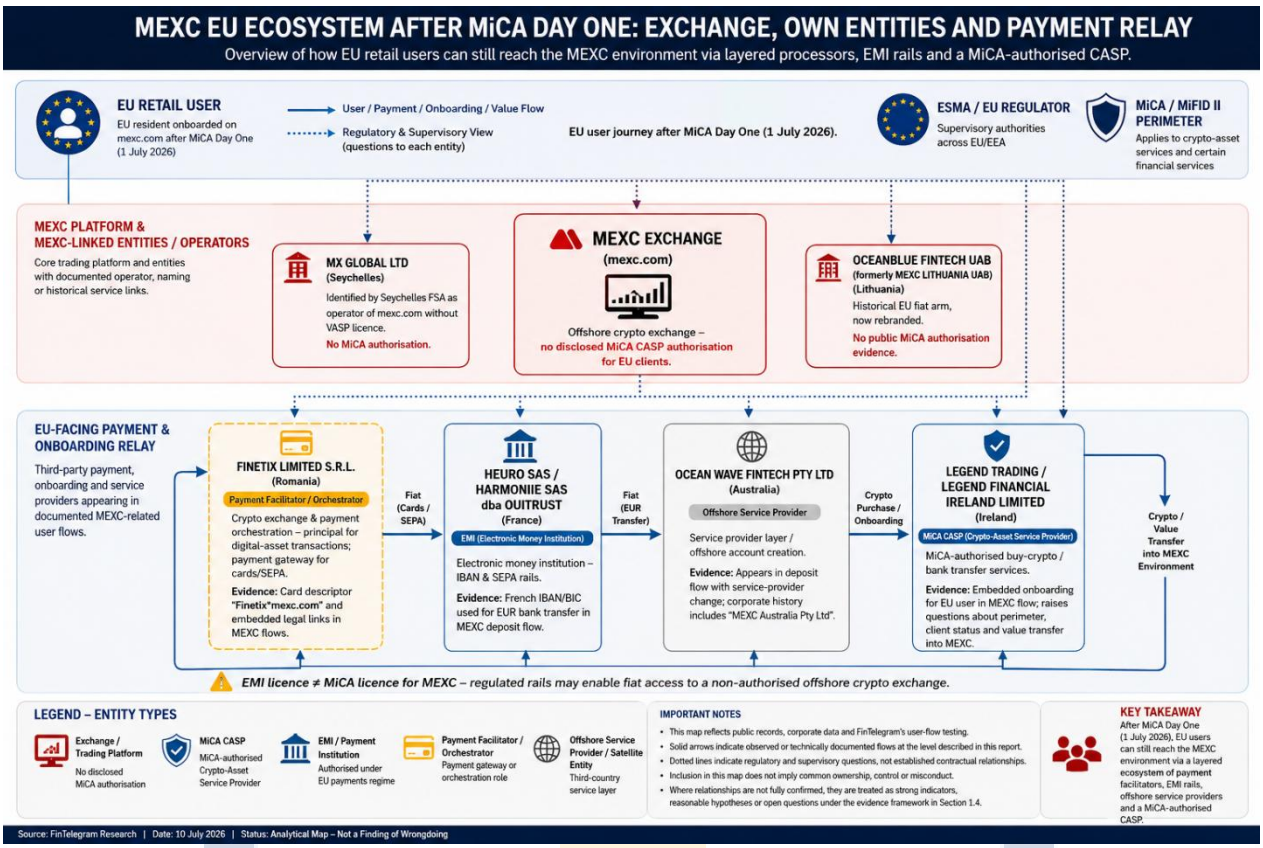

Figure 5.1 — MEXC EU Ecosystem After MiCA Day One: Exchange, Linked Entities and Payment Relay.

FinTelegram analytical map based on public regulatory records, corporate records and documented user-flow testing. Solid arrows indicate observed or technically documented user, payment, onboarding or value-flow relationships at the level described in this report. Dotted supervisory lines represent regulatory and compliance questions rather than established contractual relationships. Inclusion in the map does not imply common ownership or misconduct. Where relationships remain unconfirmed, they are treated as strong indicators, reasonable hypotheses or open questions under the evidence framework in Section 1.4.

The figure is deliberately structured around function rather than presumed ownership. It separates the MEXC platform and historically linked entities from regulated and unregulated third-party layers, because their legal positions are materially different.

5.2 How to Read the Architecture

5.2.1 The central platform layer: MEXC Exchange

At the centre of the architecture sits **MEXC Exchange (mexc.com)**, the user-facing trading environment through which FinTelegram conducted the post-MiCA onboarding and funding tests described in Section 4.

The tested EU user was able to register, complete identity and address verification, obtain functional account access and proceed toward fiat and crypto funding routes after 1 July 2026. No MiCA-

authorised MEXC entity was disclosed in the tested journey, and FinTelegram identified no MEXC entity in the MiCA register reviewed for this report.

The central compliance issue is therefore not merely that mexc.com remained technically accessible from the EU. It is the cumulative pattern of account acceptance, KYC completion, account activation and available funding functionality. In FinTelegram's assessment, that pattern is more consistent with an apparent continuation of EU-facing service availability than with a platform restricted to an orderly wind-down.

5.2.2 The operator and historically linked-entity layer

The ecosystem map distinguishes between the trading platform itself and entities with documented operator, naming or historical service links to MEXC.

- **MX Global Ltd (Seychelles)** is included because the Seychelles FSA publicly identified it as the entity operating the MEXC platform and stated that it lacked the authorisation required under the Seychelles VASP framework. This is an established regulatory fact as to the Seychelles position and materially affects the counterparty-risk profile of the platform.
- **Oceanblue Fintech UAB**, formerly **MEXC Lithuania UAB**, is included as a historical EU-facing satellite entity because previous FinTelegram reporting linked it to MEXC fiat-service arrangements under the legacy Lithuanian VASP environment. No current MiCA authorisation is established in this report.

The map does not state that all historically MEXC-branded or MEXC-associated entities form a single currently controlled corporate group. The relevant compliance point is narrower: repeated operator changes, renamings and regional service entities complicate the identification of the legal counterparty ultimately responsible for EU-facing activity.

5.2.3 Finetix: payment orchestration and gateway risk

Finetix Limited S.R.L. occupies a distinct position in the map and is therefore shown with a separate payment-orchestration risk coding rather than as a clearly regulated EU intermediary.

Finetix publicly describes itself as a crypto exchange and fiat gateway provider and states in its Terms of Use that it acts as principal in digital-asset transactions while relying on partnered payment institutions. FinTelegram's testing and earlier reporting documented several technical links between Finetix and MEXC-related flows, including:

- a card-payment descriptor associating Finetix with the MEXC domain;
- Finetix legal materials embedded in a MEXC-related user journey; and
- earlier reported SEPA and payment-account arrangements involving Finetix in MEXC-related flows.

These indicators support the working hypothesis that Finetix may perform a material orchestration or gateway role between the MEXC environment and fiat-payment infrastructure.

The precise contractual role remains unresolved. The card descriptor alone does not establish whether Finetix acts as merchant of record, sub-merchant, payment facilitator, principal, settlement beneficiary

or another form of intermediary. Those distinctions require contracts, acquirer records and settlement evidence.

5.2.4 Heuro / OuiTrust: regulated EMI rails

Heuro SAS / Harmoniie SAS, doing business as OuiTrust, is shown in blue because its position differs materially from that of an unlicensed offshore exchange. It is a French electronic money institution authorised under the French payments framework.

In FinTelegram's July 2026 testing, a MEXC-related EUR bank-transfer journey generated a concrete payment instruction using a French IBAN and Heuro banking details after the user encountered consent materials referring to the relevant service layers.

The compliance significance is not that Heuro lacks an EMI licence. Its regulated EMI status is not in dispute in this report.

The relevant issue is the boundary between the regulated payment service and the underlying crypto environment:

- Who is the legal customer of the EMI?
- On whose behalf is the IBAN or payment functionality provided?
- What counterparty due diligence has been conducted on the crypto platform behind the flow?
- How are safeguarding, complaints and AML/CFT responsibilities allocated?
- Does the payment architecture, in substance, facilitate new EU business for a non-authorised third-country crypto exchange?

An EMI authorisation does not transfer or confer MiCA authorisation on MEXC. The presence of a regulated payment rail therefore does not resolve the underlying crypto-service perimeter question.

5.2.5 Ocean Wave Fintech: service-provider migration and jurisdictional shift

Ocean Wave Fintech Pty Ltd appears in grey in the figure because its role combines a documented service-provider appearance with unresolved questions regarding current control, licensing and client treatment.

Public Australian corporate records show that the same entity previously operated under names including **MEXC Australia Pty Ltd** and **MXC Tech Pty Ltd**. During FinTelegram's tested MEXC deposit journey, a service-provider change screen indicated that the service would be provided from Australia and governed within an Australian jurisdictional context. Account-related communications were then triggered for the EU user.

This creates a material continuity and perimeter question.

The documented facts establish a historical MEXC naming connection and an appearance of the renamed entity inside the MEXC user journey. They do not, by themselves, establish current common ownership or prove that the arrangement was designed to evade MiCA.

The supervisory question is whether the mechanism represents:

- a genuine transfer to an independently entitled service provider;

- a migration of the customer relationship to a historically MEXC-linked entity;
- an offshore service layer supporting the same practical user journey; or
- another contractual structure not visible from the outside.

The distinction can only be resolved through corporate ownership records, client agreements, data-transfer arrangements and the actual flow of funds and assets.

5.2.6 Legend Trading: the MiCA-authorised layer

Legend Trading / Legend Financial Ireland Limited is shown as a regulated EU intermediary because the Irish entity holds MiCA CASP authorisation.

That authorisation materially distinguishes Legend from the other entities in the map. A MiCA-authorised CASP may lawfully provide the services covered by its authorisation to EU clients, subject to applicable passporting, conduct, AML/CFT and other requirements.

The compliance issue therefore does not arise from Legend's authorised status itself. It arises from the context in which the Legend layer appeared.

FinTelegram's testing documented a MEXC-related buy-crypto flow in which an EU user was directed into a Legend onboarding process and received related communications. This raises a set of boundary questions that are central to the ecosystem analysis:

- Is the EU user onboarded as Legend's own client?
- Which specific MiCA-authorised service is provided?
- Where does Legend's regulated service legally and operationally end?
- Where does the MEXC service begin?
- Who controls the destination account or wallet?
- Is value transferred into the MEXC environment?
- How is MEXC classified and risk-assessed as a counterparty, partner, destination platform or other participant?

The presence of a MiCA-authorised CASP inside a broader MEXC-related user journey does not itself establish a breach. It does, however, create a legitimate supervisory question as to whether regulated infrastructure is operating independently or functioning as a bridge into a non-authorised offshore exchange environment.

5.3 Supervisory Significance of the Ecosystem Model

The ecosystem view changes the compliance analysis in five important respects.

First: the relevant object of supervision is the functional architecture, not only the branded exchange

A narrow analysis focused solely on whether "MEXC has a MiCA licence" risks missing how market access may function in practice. A user may interact with one brand while separate entities perform:

- KYC or account migration;
- fiat collection;

- card acceptance;
- IBAN provision;
- crypto purchase;
- value transfer;
- settlement; or
- destination crediting.

The legal perimeter must therefore be tested against the actual allocation of functions.

Second: regulatory status does not automatically transmit through the chain

A French EMI licence authorises the regulated payment activity of the licensed EMI. It does not confer MiCA status on an offshore exchange.

Similarly, a MiCA authorisation held by an Irish CASP authorises the services of that CASP within the scope of its permission. It does not automatically regularise every platform or transaction environment into which the CASP may be embedded.

The decisive questions are therefore service-specific and entity-specific.

Third: client attribution is a core control issue

The ecosystem map exposes a recurring question:

Whose customer is the EU user at each stage of the journey?

The answer determines, among other things:

- applicable contractual rights;
- KYC responsibility;
- transaction-monitoring obligations;
- safeguarding arrangements;
- complaint handling;
- disclosures;
- data-protection responsibilities; and
- competent supervisory authority.

Where a user begins inside MEXC, accepts third-party terms, receives an IBAN from one institution, is migrated to another jurisdiction and purchases crypto through a separate CASP, the legal and operational allocation of the customer relationship becomes a central compliance issue.

Fourth: payment and onboarding intermediaries may become the practical enforcement frontier

MiCA primarily regulates crypto-asset services, but the ability of an offshore exchange to serve EU users often depends on infrastructure outside the visible trading interface.

Banks, EMIs, PSPs, CASPs, gateways, acquirers and orchestration layers may therefore become points at which the authorisation status and risk profile of the underlying crypto business must be assessed.

This does not mean that every institution appearing in a payment chain is responsible for the regulatory status of every other participant. It does mean that, where a regulated institution knowingly supports crypto-related flows, the authorisation status, enforcement history, business model and actual

economic purpose of the underlying relationship are highly relevant to a risk-based counterparty and AML/CFT assessment.

Fifth: the ecosystem creates a cumulative risk picture

No single arrow in Figure 5.1 proves a unified scheme.

The significance arises from the cumulative architecture documented around the same platform:

- continued EU onboarding after the MiCA transition deadline;
- no disclosed MEXC MiCA CASP authorisation;
- an offshore operator identified by its home regulator as unauthorised;
- historically MEXC-branded regional entities;
- a Romanian payment-orchestration layer;
- French EMI rails;
- an Australian service-provider layer with former MEXC corporate names; and
- a MiCA-authorised Irish CASP appearing in a MEXC-related user journey.

Each component must be assessed on its own evidence and legal status. Taken together, however, they justify enhanced supervisory scrutiny of the architecture as a whole.

5.4 Analytical Limitations and Evidence Boundaries

The ecosystem map is an analytical model, not a corporate-ownership chart and not a finding of coordinated wrongdoing. FinTelegram does not presently establish that:

- all entities shown contract directly with one another;
- all payment routes operate simultaneously in every user journey;
- MEXC owns or controls Finetix, Heuro/OuiTrust or Legend;
- the appearance of a regulated institution in a tested flow means that institution has breached its regulatory obligations;
- every arrow represents a completed end-to-end transfer of value; or
- the observed architecture was deliberately designed to circumvent MiCA.

Where a user flow was displayed but not completed through final settlement and account crediting, the report distinguishes the existence of the route from proof of completed value transfer.

The map should therefore be read together with the evidence framework in Section 1.4 and the entity-specific analysis that follows. Its purpose is to identify the functional architecture, separate established facts from indicators and hypotheses, and define the questions that contracts, settlement records, regulator correspondence and further whistleblower evidence must answer.

The central finding remains narrower but significant: **after MiCA Day One, a newly onboarded EU user could still access a functioning MEXC environment in which multiple payment, onboarding and service-provider layers appeared capable of supporting fiat or crypto access.**

That architecture warrants scrutiny not because every participant can be presumed to have acted improperly, but because the effectiveness of the post-transition MiCA perimeter increasingly depends on understanding how regulated and unregulated layers interact in practice.

5.5 Legacy rail: Paytend Europe UAB — and other processors observed or reported

Paytend Europe UAB (Lithuania) — the cautionary precedent

Paytend Europe UAB, a Lithuanian EMI (sole shareholder recorded in the Lithuanian registry as Junqing Li; 2024 revenue EUR 6.4 million), provided payment-account infrastructure that FinTelegram had, since May 2024, mapped inside MEXC's euro deposit rails — first via MEXC Estonia OÜ, later via Oceanblue Fintech UAB and Finetix. On 18 February 2026, FinTelegram sent Paytend's board and compliance function a formal urgent notification and open letter warning that its rails were facilitating MEXC-related deposits via Finetix. In early March 2026 the Bank of Lithuania announced the **revocation of Paytend's EMI licence** following an inspection that found serious and systematic violations in business-relationship and transaction monitoring, ML/TF risk management and internal controls — including the finding that the institution **provided the regulator with incorrect information about its business relationship with a high-risk customer and failed to retain and submit the related correspondence**, and that suspicious-transaction reports were not filed despite grounds to do so. The regulator did not name the customer, and no public finding links the high-risk customer to MEXC; the temporal and structural alignment with FinTelegram's warnings is recorded here as a **strong indicator of the risk pattern, not as an established identification**. (**Established facts** as to the inspection findings and revocation — Bank of Lithuania, notice dated 6 March 2026, services ceasing in early March 2026; LRT reporting. **Strong indicator** as to the MEXC-rail context — FinTelegram, February–May 2026.)

The Paytend precedent matters for every entity in Section 5: it demonstrates that supervisors will act against the **payment layer** of an unlicensed exchange's ecosystem, and that AML/CFT programme adequacy is judged against the real risk of the flows carried, not the nominal merchant label.

Other processors: current versus historical presence

Processor	Reported role in MEXC context	Current-flow status
OSL Pay S.R.L. (Italy)	Reported by FinTelegram (tag-page article, 2026) as a primary card gateway facilitating credit/debit card purchases for MEXC and WEEX, based on screenshots and traffic analysis, while itself applying for a MiCA licence. (Strong indicator.)	Reported in recent flows; presence in the specific 1–2 July 2026 tested journey not separately confirmed. Verification recommended.
Paytend Europe UAB (Lithuania)	EMI providing payment accounts behind MEXC euro rails via MEXC Estonia OÜ / Oceanblue / Finetix (2024–early 2026). (Strong indicator; licence revocation is established fact.)	Historical only — licence revoked March 2026; no longer able to provide financial services.

Processor	Reported role in MEXC context	Current-flow status
MoonPay; Mercuryo; Banxa; Skrill / Paysafe	Named in the commissioning brief as third-party on-ramp processors appearing in earlier MEXC-related reporting.	LEAD — VERIFICATION PENDING. FinTelegram's archive should be re-checked article-by-article before any of these names is carried into a publication version; their presence in current MEXC flows is not confirmed by the material reviewed for this report.

The pattern across the legacy and current rails is consistent: MEXC's EU fiat access has repeatedly been reconstructed around a rotating set of EU-regulated intermediaries (Estonian arm → Lithuanian EMI → Romanian gateway plus French EMI → Irish CASP layer → Australian service entity), with each reconfiguration following regulatory pressure on the previous configuration. That rotation is itself a material AML/CFT red flag for any institution asked to occupy the next slot in the chain. (**Strong indicator**, as a synthesis of the documented sequence.)

6. Legal and Compliance Assessment

6.1 MEXC's conduct measured against MiCA

Three features of the documented conduct are decisive for the MiCA analysis. **First, continued onboarding.** The 1 July 2026 test evidences acceptance, verification and activation of a new EU retail client after the end of the transitional period — conduct that ESMA's 23 June 2026 statement instructs unauthorised CASPs to cease immediately. **Second, absence of authorisation and of operator disclosure.** No MEXC entity discloses a MiCA CASP authorisation, none appears in the ESMA register as reviewed, and the tested user journey identifies no EU legal entity as service provider at all — the user contracts, in effect, with an offshore platform whose home regulator has publicly identified its operator as unlicensed. Under MiCA Article 59 read with ESMA's post-transition position, the provision of crypto-asset services to EU clients in these circumstances falls outside the authorised perimeter unless a narrow exemption applies. **Third, derivatives.** The prominent availability of futures and leveraged products to EU retail users engages the MiFID II perimeter and national CFD product-intervention measures independently of MiCA, as the Belgian FSMA's 2024 order already illustrated at Member-State level.

The principal defence available to MEXC would be **reverse solicitation**. On the documented record it appears weak: the platform actively verified an EU address, granted account functionality, listed EU countries in its own deposit-support materials and embedded EU payment rails in its flows — indicia of servicing and soliciting an EU market rather than passively responding to a client's exclusive initiative. A second possible position — that EU users are contractually migrated to third parties (Ocean Wave, Legend) and therefore are no longer MEXC's clients — raises rather than answers the perimeter question, since ESMA has made clear that client transfers require the receiving provider to be entitled to serve those clients and that outsourcing and B2B constructions do not exempt non-EU CASPs. Both defences are noted as **open questions** on which MEXC's response is invited; neither is visible, let alone substantiated, in the tested journey.

6.2 Payment-facilitator exposure: the questions every institution in the chain must answer

For Finetix, Heuro/OuiTrust, Legend, Ocean Wave, and any EMI, PSP, bank or card acquirer appearing in MEXC-related flows, the supervisory analysis reduces to three questions. **(i) Enablement:** does the institution's service, in substance, enable a non-authorised CASP to continue EU business after 1 July 2026 — for example by providing the IBAN into which new EU customers pay, the card acceptance behind a Finetix*mexc.com descriptor, or the regulated on-ramp inside the exchange's deposit flow? (ii) Perimeter due diligence: has the institution demonstrably assessed MEXC's MiCA status, the ESMA register position, the FCA/FSMA/ASIC/AFM warnings and the Seychelles FSA enforcement action — all public — and documented a reasoned decision about the relationship? An institution that cannot evidence such an assessment after MiCA Day One is exposed to the charge that its counterparty risk framework is not commensurate with its actual risk. (iii) AML/CFT adequacy:** are onboarding, transaction monitoring, STR practice and governance adequate for flows connected to a platform with this warning history? The Paytend revocation demonstrates the

supervisory consequence of answering these questions badly: the Bank of Lithuania's findings centred precisely on monitoring, high-risk-customer handling and internal controls.

None of this presumes the answer for any particular institution. A regulated firm may be able to show that it onboards each EU user as its own client with full disclosures, that it has classified the exchange-related flows correctly, and that its regulator is informed. The purpose of this report is to put the questions on the record — and to enable supervisors to ask them.

6.3 Risk-matrix narrative

The following matrix expresses FinTelegram's assessment of **regulatory exposure** — the likelihood that the entity's documented position attracts supervisory scrutiny or action — on a Low / Medium / High scale. It is an analytical opinion based on the evidence tiers stated in this report, not a legal finding, and each rating is revisable upon the entity's response.

Entity	Exposure	Basis (cautious formulation)
MEXC operator entities (MX Global Ltd; platform operators)	High	Documented post-deadline EU onboarding with no disclosed authorisation; home-regulator enforcement; multi-jurisdiction warnings; retail derivatives offering. Exposure spans MiCA, MiFID II/product intervention and national regimes.
Finetix Limited S.R.L.	High (pending clarification)	Card descriptor and payee evidence placing it at the centre of MEXC's EU fiat flows; self-description as crypto exchange and fiat gateway acting as principal; no identified MiCA authorisation. Rating would change materially if Finetix evidences authorisation, a compliant perimeter analysis, or termination of the flows.
Heuro SAS / Harmoniie SAS dba OuiTrust	Medium-to-High	Authorised EMI whose rails appear inside a non-authorised exchange's post-MiCA deposit flow; prior external reporting and published rebuttal; questions of customer attribution, safeguarding and ML/TF risk assessment outstanding. EMI authorisation itself is not in doubt.
Ocean Wave Fintech Pty Ltd	Medium-to-High	Established MEXC-name corporate history on the same ABN; automatic in-flow migration of EU users to Australian law days after the MiCA deadline; independence, licensing and AML posture unclarified. Rating reflects unresolved linkage, not any established breach.

Entity	Exposure	Basis (cautious formulation)
Legend Trading / Legend Financial Ireland Ltd	Medium	MiCA-authorised CASP — the strongest regulatory position in the chain — but embedded inside an unauthorised exchange's user journey, raising perimeter, outsourcing, client-attribution and due-diligence questions that merit clarification to its supervisor.
OSL Pay S.R.L.	Medium	Reported card gateway for MEXC and WEEX while itself a MiCA applicant; the compliance tension between applicant status and servicing non-MiCA exchanges warrants clarification. (Secondary-source basis; verification recommended.)
Paytend Europe UAB	Realised	EMI licence revoked March 2026 for serious and systematic AML/CFT and internal-control failures — the precedent case for payment-layer exposure in this ecosystem.
Card acquirers, scheme members and banks behind the descriptors and IBANs	Medium	Exposure depends on whether merchant classification, MCC coding, descriptor transparency and counterparty due diligence reflect the true crypto counterparty; unidentified pending evidence.

7. Open Questions and Information Gaps

The following points cannot be resolved from public sources or platform testing. They define the evidentiary frontier of this investigation; only contracts, internal records, whistleblower material or regulatory disclosure can close them.

- **Contractual architecture.** The actual agreements between MEXC entities and, respectively, Finetix, Heuro/OuiTrust, Ocean Wave and Legend: who contracts with whom, in what capacity (merchant of record, principal, agent, liquidity provider, outsourced service provider), and under which governing law.
- **Beneficial ownership and control.** The ultimate ownership of MX Global Ltd and the wider MEXC platform; of Finetix Limited S.R.L.; of Ocean Wave Fintech Pty Ltd; and of EasyEuro Technology Limited (HK) as shareholder of Heuro SAS — and whether any ownership, funding, management or profit-sharing links exist between MEXC and any rail entity. No common ownership is alleged; the question is open in both directions.
- **Flow of funds.** The complete settlement chain from the EU payer's euros (via Heuro IBAN or Finetix card descriptor) to the crediting of value inside MEXC — including any conversion through the HEURO e-money token or other stablecoins, correspondent accounts used, and the identity of acquirers and scheme members.
- **Client attribution and data sharing.** Whose customer the EU user legally is at each step; what KYC data MEXC shares with Ocean Wave, Legend, Finetix or Heuro (the automatic account creations suggest data transfer whose GDPR basis is unexplained); and what disclosures the user actually receives.
- **Outsourcing and perimeter design.** Whether any layer was structured on legal advice specifically to navigate the MiCA perimeter; whether Legend's role is documented internally as outsourcing, client acquisition or independent service; and whether Ocean Wave's service-provider change is a genuine novation or a jurisdictional relabelling.
- **Regulator awareness.** Whether the ACPR, the Central Bank of Ireland, the BNR/Romanian FIU, AUSTRAC/ASIC, or any NCA has been notified of, or has reviewed, the respective MEXC relationships; and whether STRs relating to these flows have been filed by any institution in the chain.
- **Historical processors.** Confirmation, from FinTelegram's own archive and from the processors named, of the historical and current presence of OSL Pay, MoonPay, Mercuryo, Banxa and Skrill/Paysafe in MEXC flows (see Section 5.5 — partially LEAD status).
- **Scale.** Volumes of EU-origin fiat entering the MEXC environment post-1 July 2026, by rail and by month — the single most important quantitative gap for supervisory prioritisation.

8. Questions for Stakeholders and Right-of-Reply Framework

FinTelegram addresses the following neutral clarification questions to the named entities. All addressees are invited to respond to any and all questions; responses, corrections and substantiated objections will be reflected in updated versions of this report and in derived FinTelegram publications. Silence will be noted as such, without adverse inference being stated as fact.

8.1 To MEXC and MEXC-linked entities (incl. MX Global Ltd)

1. Which legal entity provides crypto-asset services to EU residents on mexc.com as of 1 July 2026, and under which authorisation?
2. Does any MEXC-linked entity hold, or has any applied for, a MiCA CASP authorisation? If an application is pending, before which NCA?
3. Why could a new EU resident register, complete advanced KYC and receive deposit access and a 200 BTC withdrawal limit on 1 July 2026?
4. Does MEXC consider its EU-facing services to be reverse-solicited? On what factual basis, given EU-country deposit support pages and embedded EU payment rails?
5. What is the contractual role of Finetix, Heuro/OuiTrust, Ocean Wave and Legend Trading in MEXC's EU fiat flows?
6. Why does Ocean Wave Fintech Pty Ltd — with prior names MEXC Australia Pty Ltd and MXC Tech Pty Ltd — appear as incoming service provider for EU users, and what happens to users who reject the change?
7. Which entity provides custody of EU users' assets, and how is that reconciled with MiCA's restrictions on custody by, and delegation to, non-CASPs?
8. On what basis are futures and leveraged derivatives offered to EU retail clients in light of MiFID II and national product-intervention measures?
9. What wind-down measures, if any, has MEXC taken for its EU business, and where are they communicated to users?

8.2 To Finetix Limited S.R.L.

10. Is Finetix a contractual partner, payment facilitator, merchant of record, principal, liquidity provider or settlement agent for MEXC or MEXC-linked entities?
11. Why does a card transaction in the MEXC flow carry the descriptor Finetix*mexc.com, and which acquirer and scheme arrangements stand behind it?
12. Does Finetix process fiat inflows for MEXC EU users, and in what volumes since 1 July 2026?
13. Has Finetix assessed whether MEXC holds a MiCA CASP authorisation, and what was the outcome and documentation of that assessment?
14. Under which authorisation does Finetix itself provide crypto exchange and fiat gateway services to customers across European jurisdictions, acting as principal?

15. Which partnered payment institutions does Finetix use for MEXC-related EUR flows, now that Paytend's licence has been revoked?
16. Has Finetix notified Romanian authorities or any EU regulator of the MEXC relationship, and has it filed suspicious-transaction reports in connection with these flows where warranted?

8.3 To Heuro SAS / Harmoniie SAS, dba OuiTrust

17. Does Heuro/OuiTrust provide IBAN, SEPA, e-money or other payment services used in MEXC-related deposit flows? If so, under which contractual relationship — with Finetix, with a MEXC entity, or with another party?
18. Is Finetix a client, partner or intermediary of Heuro/OuiTrust, and what due diligence has been performed on the end-flows behind Finetix?
19. Whose customer is the EU payer in the tested flow — Heuro's, Finetix's, MEXC's, or another party's — and which safeguarding and complaint-handling framework applies to their funds?
20. Has Heuro/OuiTrust assessed MEXC's MiCA authorisation status and its public warning and enforcement record, and with what documented conclusion?
21. Does Heuro/OuiTrust permit its EMI rails, or the HEURO e-money token, to be used for inflows to crypto exchanges without MiCA authorisation, and what controls apply?
22. Has Heuro/OuiTrust notified the ACPR or Banque de France of MEXC-related flows, and have STRs been filed with Tracfin where warranted?
23. Is there any ownership, funding, management or commercial link between Heuro/OuiTrust or EasyEuro Technology Limited and MEXC or MEXC-related entities?

8.4 To Ocean Wave Fintech Pty Ltd

24. What is the current relationship between Ocean Wave and MEXC, and who are Ocean Wave's beneficial owners?
25. Why did the company previously operate as MEXC Australia Pty Ltd and MXC Tech Pty Ltd, and when and why did the current name and any change of control take effect?
26. Does Ocean Wave provide services to EU users routed through mexc.com, and does it consider those users to fall outside the EU regulatory framework once the service-provider change is accepted?
27. Is Ocean Wave registered with AUSTRAC for digital-currency-exchange services, and does it hold any AFSL or other ASIC authorisation relevant to the services provided?
28. Does Ocean Wave conduct its own KYC, AML and sanctions screening on migrated EU users, or does it rely on MEXC's verification, and on what legal basis is user data transferred to it?
29. Does Ocean Wave hold or control customer fiat or crypto assets, and under which safeguarding arrangements?
30. What happens, contractually and operationally, to a user who rejects the service-provider change?

8.5 To Legend Trading / Legend Financial Ireland Limited

31. Does Legend provide services to users arriving through embedded MEXC flows, and is MEXC (or any MEXC-linked entity) a partner, platform, merchant or counterparty of Legend?
32. Is the EU user onboarded as Legend's own client, with full MiCA conduct, disclosure and asset-protection obligations attaching? Which entity is the client-facing CASP of record?
33. Does Legend transfer purchased crypto-assets or liquidity into the MEXC environment, and under what counterparty classification and due-diligence framework?
34. What due diligence has Legend conducted on MEXC's MiCA status, its regulatory warnings and the Seychelles FSA enforcement action, and what was the documented conclusion?
35. Has Legend assessed the arrangement against ESMA's statements on non-EU CASPs, reverse solicitation and prohibited outsourcing or delegation, and has the Central Bank of Ireland been informed of the MEXC-related flows?
36. Which crypto-asset services on Legend Financial Ireland Limited's authorisation schedule are engaged by the MEXC-embedded flow, and in which Member States is passporting effective?

8.6 To EMIs, PSPs, banks and card acquirers appearing in the flows

37. Do you provide accounts, acquiring, issuing, settlement or correspondent services connected to Finetix, Heuro/OuiTrust, Ocean Wave, Legend or MEXC-related descriptors and IBANs?
38. How are these merchants and counterparties classified in your systems (MCC, risk rating), and does that classification reflect the crypto-exchange nature of the underlying flows?
39. Have you screened these flows against the ESMA MiCA register and public warnings concerning MEXC, and with what documented outcome?
40. Have you filed suspicious-transaction or suspicious-activity reports connected to these flows where warranted, and have you informed your competent authority of the relationship?
41. What enhanced due diligence applies to descriptor constructions of the form Processor*platform-domain, where the platform is an unauthorised third-country exchange?

9. Call for Whistleblowers and Evidence Guidelines

FinTelegram invites current and former employees, contractors, compliance officers, MLROs, users, payment processors, EMIs, PSPs, acquirers, banking partners, auditors, market makers, affiliates and regulators with knowledge of MEXC, Finetix, OuiTrust/Heuro, Ocean Wave Fintech, Legend Trading, Paytend, OSL Pay or any related EU fiat rail to contact FinTelegram through its **Whistle42** whistleblower platform.

9.1 What is most useful

- **Contracts and commercial documents**: service, merchant-of-record, orchestration, liquidity, outsourcing or referral agreements between any of the named entities; fee schedules; side letters.
- **Internal communications**: e-mails, chats or memoranda discussing MiCA status, EU market access, reverse solicitation, entity renaming, the service-provider change, or the design of the post-Paytend rail.
- **Compliance records**: risk assessments, counterparty due-diligence files, onboarding decisions, escalations, board or committee minutes, and internal or external audit findings concerning MEXC-related flows.
- **Transactional evidence**: settlement reports, descriptor and MCC configurations, IBAN allocations, volumes of EU-origin flows, and treasury or stablecoin conversion records.
- **Regulatory interactions**: correspondence with the ACPR, Central Bank of Ireland, Bank of Lithuania, BNR, AUSTRAC/ASIC or any NCA; SAR/STR filings connected to these flows (where lawfully shareable in your jurisdiction — see caution below).
- **User-journey evidence**: screenshots, e-mails and account records documenting onboarding, deposits, service-provider changes and disclosures.

9.2 How evidence is handled

Submissions via Whistle42 can be made confidentially. FinTelegram protects sources as a matter of principle and of journalistic law: identities are not disclosed, published material is redacted of source-identifying details, metadata is removed before any publication, and documents are used in publications only in anonymised or summarised form unless the source expressly agrees otherwise. Where material supports supervisory action, FinTelegram may — only with the source's consent — facilitate contact with the competent authorities. **Important caution:** the tipping-off and disclosure rules of your jurisdiction may restrict sharing of SAR/STR material specifically; prospective sources should not breach such rules and may instead describe the existence and subject-matter of filings in general terms or seek legal advice. FinTelegram does not solicit the violation of any legal obligation; it solicits lawful accountability.

10. Principal Sources

10.1 Primary sources (regulators, registers, official statements)

- ESMA, Public Statement on unauthorised CASPs and the end of the MiCA transitional period, ESMA75-113276571-1710, 23 June 2026; ESMA Statement on the end of transitional periods under MiCA, ESMA75-113276571-1679, 17 April 2026; ESMA statement of 4 December 2025.
- Regulation (EU) 2023/1114 (MiCA), notably Articles 59, 60–64 and 143(3); Regulation (EU) 2023/1113 (Transfer of Funds recast).
- FCA Warning List: MEXC Global Ltd — https://www.mexc.com/ (unauthorised firm).
- ASIC / MoneySmart Investor Alert List: MEXC Global (www.mexc.com).
- FSMA (Belgium), Order against Mexc Global LTD (www.mexc.com), published July 2024.
- Financial Services Authority of Seychelles, enforcement announcement of 26 May 2026 identifying MX Global Ltd (IBC 238047); press releases of 14 February 2025 and 30 May 2025 concerning MEXC Global LTD (IBC 218833).
- Bank of Lithuania, PAYTEND EUROPE, UAB has lost its licence, notice of 6 March 2026 (services ceased early March 2026).
- Australian Business Register, ABN 59 638 473 211 (Ocean Wave Fintech Pty Ltd; prior names Ocean Waive Fintech Pty Ltd, MEXC Australia Pty Ltd, MXC Tech Pty Ltd).
- ACPR / company legal disclosures: Harmoniie SAS / Heuro SAS dba OuiTrust, EMI licence no. 17478, BIC HRSAFR22, 1 Rue de la Bourse, 75002 Paris.
- Central Bank of Ireland registers; Legend Trading announcements of 25 November 2024 (VASP registration) and 13 October 2025 (MiCA CASP authorisation of Legend Financial Ireland Limited); Fintech Ireland, October 2025.
- Finantsinspektsioon / Estonian FIU announcement of 30 June 2026 on the end of the Estonian transitional period (contextual).

10.2 Investigative secondary sources

- FinTelegram, MiCA/MiFID-II Perimeter Radar: MEXC Still Onboards EU Users On MiCA Day One, 1 July 2026.
- FinTelegram, MEXC Update: The Finetix–OuiTrust–Ocean Wave–Legend Trading Payment Relay Exposed, 2 July 2026.
- FinTelegram, COMPLIANCE ALERT: The MEXC Euro-Asian Shadow Rail with French Heuro & Romanian Finetix, February 2026; Open Letter to Paytend Europe UAB, 18 February 2026; Paytend EMI Licence Revoked — MEXC Rail Scrutiny Intensifies, May 2026.
- FinTelegram, MEXC Compliance Update — Red-Flag Warning, 28 October 2025 (incl. Oceanblue Fintech UAB / MEXC Lithuania UAB; MEXC Estonia OÜ); further articles under fintelegram.com/tag/mexc, including the OSL Pay card-gateway report.
- FinTelegram, MiCA Day One: FinTelegram Launches The MiCA/MiFID-II Perimeter Radar, 1 July 2026; Estonia Pulls The Plug On The Old Crypto Licence Era, July 2026.

- The Big Whale, EXCLUSIVE — HEURO: The Dark Side of the €600 Million Stablecoin, April 2026, and Heuro's published response thereto.
- LRT (Lithuania), Bank of Lithuania revokes e-money license of Chinese-owned Paytend Europe, March 2026.
- Comsure Group summary of the Seychelles FSA action (incl. AFM warning reference), May–June 2026; The Full FX, ESMA Serves Time on Unauthorised Crypto Providers, 25 June 2026 (Kaiko conversion data).
- Corporate self-descriptions as reviewed: finetix.net; ouitrust.com; heuro.com; harmoniiesas.eu; legendtrading.com; oceanfinance.online; mexc.com support pages and User Agreement.

Disclaimer: FinTelegram is an independent cyberfinance intelligence and compliance platform. This report is provided for informational, regulatory and compliance purposes only; it does not constitute legal or investment advice and does not allege criminal conduct by any person or entity. All named parties are invited to submit corrections and statements, which will be published and incorporated. Version 1.0, 4 July 2026.