pescheck

INDUSTRY BRIEF

Personnel Screening in Fintech & Financial Services

How regulated financial organisations can hire faster without lowering the integrity bar.

Fintech

Crypto

Banking

Payments & E-Money

Insurance & Wealth Management

Jump TRADING

Atradius Managing risk, enabling trade

中国银行 BANK OF CHINA

unzer

insify

Swiss Re

surepay

Europe's Financial Sector is Hiring at Speed in its Most Sensitive Roles

European financial services are absorbing the largest wave of regulation in a decade. DORA has applied since 17 January 2025, and the EU AML package, with its single rulebook and new supervisory authority AMLA, applies from 10 July 2027.[13][15] Each of these regimes ends up as a hiring requirement: more compliance, risk, security and engineering staff, each with access to customer data, funds or critical systems.

Numbers

The talent market is straining to keep up. In PwC's 2026 EMEA AML Survey of 531 financial institutions, only about one third of EU respondents expect to be compliant with the AML package by the July 2027 deadline. Up to 35% struggle to recruit qualified staff, and up to 22% expect to lose people to AMLA itself.[1] 86% of compliance professionals already describe their department as understaffed.[2]

The technology side is just as tight. Europe faces a shortfall of more than 300,000 cybersecurity professionals, and DORA has added a second layer of demand for security leaders who understand ICT risk, outsourcing and incident governance.[3] The gap is widest for exactly the profiles with the most access: AML and KYC analysts, transaction-monitoring specialists, cloud and security engineers, and payments operations staff.

At the same time, the threat has moved inside. In May 2025, Coinbase disclosed that criminals had paid overseas customer-support agents to copy customer data out of internal tools, and estimated the cost of remediation at $180–400 million.[4] Close to 70,000 customers were affected, and the data had been leaking since December 2024.[5]

Coinbase's CEO later said support agents were being offered bribes of up to $250,000.[6] In February 2026, a former TD Bank employee pleaded guilty to taking bribes for confidential customer information that enabled more than $500,000 in fraud.[7]

Hiring itself has become an attack vector. In June 2025, US prosecutors charged four North Koreans who used stolen and fabricated identities to get developer jobs at an Atlanta blockchain company and a Serbian crypto-token firm, then stole roughly $900,000 in digital assets.[8] The US Department of Justice has separately sought forfeiture of $7.74 million in stablecoin wages that blockchain firms paid to North Korean IT workers hired under false identities.[9] One security researcher estimated in November 2025 that up to 20% of crypto companies may unknowingly have North Korean workers embedded.[10] The control that failed in these cases was identity and integrity verification at the point of hire, not the firewall.

The Candidate Side of the Market

The candidate side is shifting too. In a 2025 Gartner survey of 3,000 job candidates, 6% admitted to interview fraud, either posing as someone else or having someone else pose as them. Gartner predicts that by 2028, one in four candidate profiles worldwide will be fake.[11] For a payments firm or a crypto platform, a fake candidate is not just a bad hire: it is a person with credentials to customer accounts, transaction systems or wallets.



The result is a squeeze every HR and compliance lead in this sector recognises: hire faster than ever, into roles with direct access to customer data and money, with a supervisor watching every appointment.

Why Screening is Now a Compliance Requirement, not a Nice-to-Have

For banks, payment and e-money institutions, crypto-asset service providers, insurers and investment firms, personnel screening sits at the intersection of several regulatory regimes at once:

- **DORA, Regulation (EU) 2022/2554.** DORA has applied since 17 January 2025 and, for financial entities, takes the place NIS2 holds in other sectors. Its ICT risk-management standard (Commission Delegated Regulation (EU) 2024/1774, Article 19) requires financial entities to build ICT security into their HR policy, covering both their own staff and the staff of ICT third-party providers who access their ICT assets.[13] DORA does not prescribe a checklist; in practice it means verification proportionate to the access granted, completed before access, and evidence a supervisor can inspect.

- **The EU AML package:** AMLR, Regulation (EU) 2024/1624, Article 13. From 10 July 2027, every employee, agent or distributor directly involved in AML/CFT compliance must undergo a risk-proportionate assessment of skills, knowledge, good repute, honesty and integrity before taking up the role, and regularly thereafter. The content of that assessment must be approved by the compliance officer, and staff must disclose close relationships with customers.[14][15] This applies to crypto-asset service providers as well as banks and payment firms.

- **National integrity screening.** In the Netherlands, a bank may only appoint someone to an integrity-sensitive position after a substantiated assessment of that person's reliability. In practice this is a pre-employment screening whose depth matches the risks of the role, followed by periodic sanctions checks on existing staff.[17] Other member states have comparable rules.

- **ISO/IEC 27001:2022, control A.6.1.** Background verification must be carried out on all candidates before joining and on an ongoing basis, proportional to the classification of information accessed and the perceived risks.[18] Auditors expect a screening policy, a role risk-classification matrix and a documented screening record per person.

- **GDPR.** All of the above must be lawful, data-minimised and defensible, with particular care around criminal-record data under Article 10 and around financial checks, which must be justified by the role.

Screening here has to satisfy two audiences that usually pull in opposite directions: compliance and risk teams who want depth and evidence for the supervisor, and hiring managers who cannot afford to lose a scarce AML analyst or security engineer because vetting took three weeks.

Matching Screening Depth to Role Risk



Screening depth: Standard

Backend engineer at a payments scale-up

This engineer works on the payment platform's code and has access to staging and selected production systems, but not to customer funds or accounts directly. The main risks are a misrepresented identity or skill set, including fake remote candidates, and source code or IP leaving with a departing employee.

Screening: identity and biometric verification, education verification, employment history, references, a VOG with a role-appropriate screening profile, and a sanctions check.



Screening depth: Integrity-sensitive

KYC/AML analyst or customer-support agent

This employee can see customer identities, account data and transaction histories, and may be able to approve onboarding or clear alerts. The key risks are bribery, sale of customer data, collusion with criminals and undisclosed relationships with customers.

Screening: the standard package, plus in-depth sanctions and PEP screening, an adverse media check, an integrity and conflict-of-interest declaration, proportionate a financial check, and periodic re-screening.



Screening depth: Enhanced

Head of Compliance, MLRO or digital-asset custody lead

This person is a key function holder or controls the systems that move client money and crypto assets. The key risks are an undisclosed regulatory or criminal history, past directorships of failed or sanctioned entities, and financial vulnerability.

Screening: the integrity-sensitive package, international criminal record checks for previous countries of residence, directorship, bankruptcy and register checks, extended references from previous regulated employers, and ongoing monitoring.

What is Actually Possible to Verify

A well-designed programme starts from the risk, not the check. Every role carries a baseline risk of misrepresented identity, qualifications or work history. Integrity-sensitive roles add exposure to bribery, data theft and conflicts of interest. Key function holders add regulatory history and financial vulnerability.

Each tier therefore gets a different depth of screening, matched to what could actually go wrong in that role. Pescheck supports the full range, from standard verification to in-depth checks for the most sensitive positions.[19]

- Identity fraud → Identity & biometric verification
- Insider / integrity risk → Integrity declaration, adverse media
- Export-control exposure → Relevant declarations and documentation
- Qualification risk → Education and certification verification
- Experience risk → Employment and reference verification
- Sanctions exposure → Sanctions / PEP / watchlist screening
- Ongoing personnel risk → Periodic or event-based re-screening

The Pescheck Case

The challenge our customers brought us

- Supervisory expectations from DNB, AFM and other national authorities, plus fit-and-proper files for key function holders
- High hiring volume in operations, KYC and customer support across multiple countries, entities and licences
- Manual, decentralised screening that differed by business unit and did not scale with growth
- Bank partners, auditors and supervisors demanding full traceability of who has access to what
- Compliance obligations spanning DORA, the AML package, national integrity rules and ISO 27001 simultaneously

What we implemented

- Standardised screening workflows per role tier, so the same evidence is collected the same way in every country and entity
- Integrity-focused check packages covering identity, sanctions and PEP screening, adverse media, integrity declarations and fit-and-proper documentation
- ATS and HR system integration, alongside 100+ other integrations and a full API, so screening starts automatically from the existing recruitment process [19]
- Centralised dashboard with live status per candidate, structured decision-making and a complete audit trail
- EU-built, EU-hosted infrastructure, ISO 27001 and NEN 7510 certified, POB/WPBR registered and PBSA affiliated [20]

The outcome

- Designed to support a compliant, audit-ready screening process, with each step documented so decisions can be explained to supervisors, auditors and bank partners
- Average turnaround of under 4 hours, against hiring cycles measured in weeks [19]
- A consistent screening standard across teams, entities and countries, helping reduce variation between divisions
- More than 300,000 screenings performed on our technology for 2,600+ organisations [19]

Why it Matters Commercially, not Just Legally

Screening is increasingly a condition of doing business in this sector. Sponsor banks and Banking-as-a-Service partners audit the fintechs they work with, supervisors ask for evidence during licence applications and on-site inspections, and under DORA every financial entity must manage the risk of its ICT providers, so fintech vendors are asked how their own staff are vetted. Investors in payments and crypto ask the same question during due diligence. At the same time, you need to hire scarce compliance and engineering talent quickly, before they accept another offer. PESCHECK sits exactly between those two needs. A documented, standardised programme keeps hiring moving and turns a compliance cost into a credential you can put in front of a bank partner or a supervisor.

The economics hold up independently. Around 10% of candidates show a background discrepancy, and a bad hire can cost up to 2.5x their salary,[19] before accounting for a regulatory finding, a lost banking partner or a licence put at risk. At the extreme end, a data breach in financial services costs an average of $5.56 million, and breaches started by malicious insiders are the most expensive category of all.[12] Speed matters, but not at the expense of integrity.

Organisations in this sector working with Pescheck include [customer names to confirm - e.g. banks, payment institutions, crypto-asset service providers, insurers].

Jump TRADING

Atradius
Managing risk, enabling trade

中国銀行 BANK OF CHINA

unzer

insify

surepay

Swiss Re



Sources

1. PwC Luxembourg, EMEA AML Survey 2026 (April 2026) — 531 institutions; about one third of EU respondents expect AML-package readiness by July 2027; up to 35% struggle to recruit; up to 22% expect to lose staff to AMLA.

2. Barclay Simpson, 2025 Salary Survey & Recruitment Trends Guide: Compliance & Financial Crime — 86% of professionals believe their compliance department is understaffed.

3. Optima Europe, European Cybersecurity Talent Market 2026 — shortfall of 300,000+ cyber professionals; DORA-driven demand in financial services.

4. CNBC, Coinbase says hackers bribed staff to steal customer data and are demanding $20 million ransom (May 2025) — bribed overseas support agents; $180–400m estimated cost.

5. The Register, Coinbase confirms insiders handed over data of 70K users (May 2025) — ~70,000 customers; breach began 26 December 2024.

6. Bitdefender, Coinbase insider who sold customer data to criminals arrested in India — bribes of up to $250,000 offered to support agents.

7. IRS Criminal Investigation, Bank insider pleads guilty to facilitating fraud schemes from inside two financial institutions (February 2026) — former TD Bank employee; bribes for customer data; $500,000+ fraud.

8. US DOJ, Four North Koreans charged in nearly $1 million cryptocurrency theft scheme (June 2025); summary via CAFC — Atlanta blockchain firm and Serbian token company.

9. Decrypt, DOJ seeks $7.7 million forfeiture in crypto from North Korean hackers masquerading as IT workers — wages paid in stablecoins by blockchain firms.

10. crypto.news, North Korea has infiltrated up to 20% of crypto firms, security expert says (November 2025) — single-expert estimate; treat as indicative.

11. Gartner, Survey shows just 26% of job applicants trust AI will fairly evaluate them (July 2025) — 6% admitted interview fraud; 1 in 4 candidate profiles fake by 2028.

12. IBM / Ponemon, Cost of a Data Breach Report 2025, summarised by Baker Donelson — financial services $5.56m average; malicious insider attacks the costliest initial vector ($4.92m).

13. Springlex, DORA RTS on ICT risk management (CDR (EU) 2024/1774), Article 19 – Human resources policy.

14. Springlex, AMLR (Regulation (EU) 2024/1624), Article 13 – Integrity of employees.

15. Osborne Clarke, Key implications of the AMLR for financial institutions' AML policies — AMLR applies from 10 July 2027; employee integrity assessment before and during the role.

16. EBA/ESMA, Joint Guidelines on the assessment of suitability (EBA/GL/2021/06); 2026 consultation on revised guidelines (EBA/CP/2026/03).

17. Dutch Minister of Finance, letter to the House of Representatives, Kamerstuk 31477 nr. 40 (June 2019) — integrity-sensitive positions; pre-employment screening matched to role risk; periodic sanctions checks.

18. ISMS.online, ISO 27002:2022 Control 6.1 – Screening.

19. Pescheck, platform capabilities and figures — 100+ integrations and API, <4h average turnaround, 300,000+ screenings, 2,600+ organisations, ~10% discrepancy rate, bad hire up to 2.5x salary (figures carried over from the defence brief; confirm before publishing).

20. Pescheck, certifications — ISO 27001, NEN 7510, POB/WPBR, PBSA (replace with a financial-services industry page if one exists).