The Worldline Fraud Scandal: How Europe's Payment Giant Allegedly Enabled Billions in Scams From High-Risk Merchants

Many of their high-risk merchants came from Wirecard

On June 25, 2025, shares of French payment processor Worldline SA plunged 41% to an all-time low, wiping out over €500 million in market value in a single day.

The reason for that massive drop was "Dirty Payments," an nvestigation by 21 European media outlets coordinated by the European Investigative Collaborations (EIC) network. That article revealed how one of Europe's largest payment companies allegedly enabled billions of euros in fraud while systematically concealing it.

Worldline allegedly processed payments for high-risk merchants like pornography networks, illegal casinos, subscription scams, and fraudulent dating sites even after explicit warnings from Visa and multiple European regulators.

They Used A Scheme Called Division Shuffling

At the heart of the scandal was a “division shuffling” scheme. According to NRC, when one Worldline division accumulated too many fraudulent customers, they were simply "shifted to another division" to artificially lower fraud percentages.

This practice allowed the company to continue processing payments for merchants that other payment processors had terminated.

In 2020 for example, when Worldline's risk committee recommended terminating relationships with problematic clients, the commercial division objected, and pointed to the fact that they would lose $41.8 million in revenues if they did that. The decision was made to retain the clients.

The investigation alleged that many of the most problematic merchants that Worldline processed for were Wirecard refugee merchants that lost processing when Wirecard went out of business.

Some Of The More Notable Merchant Groups Mentioned

Some of their most notable high-risk merchants included the following:

#1 - The Aether Group: A Global Scam Empire Linked To QR Phishing

The investigation featured the Aether Group, a Dubai-based entity that operated over 1,000 websites through 300 shell companies. The company used to be known as Linkmedia, and was classified as "high-risk" by Worldline but continued processing nearly £50 million in 2023.

The Aether network specialized in deceptive subscription models. A prime example is inn2flix.com, presented as a film and TV download service but it was actually nothing but a subscription trap.

Victims were often lured through QR code parking scams or social media ads promising free iPhones. One scheme generated £3.5 million in losses across nearly 800 reported cases.

#2 - The Ruben Weigand Portfolio: Pornography Merchants Linked To Fraud

Another major focus was the portfolio of 311 high-risk merchants referred to Worldline's German subsidiary Payone, by consultant Ruben Weigand, who was previously convicted in the United States for conspiracy to commit bank fraud.

The portfolio consisted primarily of pornography and dating websites which were linked to fraudulent use of credit cards.

#3 – Emerchantpay – Fast Tracking High Risk Merchants

Emerchantpay (EMP), a British payment intermediary, received what investigators called an "exception position" even though they were considered a very high risk.E EMP worked to provide high risk merchants to Worldline and they were able to get fast-track approval.

EMP accounted for 40% of fraud cases in one Worldline division but was exempted from stricter control measures. This was suspicious.

Even more damning, documents from 2020 show Worldline specifically asked EMP to help with "cleaner transactions (for example load balancing) to lower reported fraud ratios. In the US the practice of microtransactions on prepaid debit cards is often used for this.

Types of Risk Activity Alleged

Based on the Worldline investigation documents, here are 10 bullet points of the most-risky merchant behaviors:

- **Daily multiple card abuse** - The same credit card being used multiple times per day across numerous different websites in the same merchant network, a classic money laundering pattern
- **Subscription trap operations** - Setting up fake services like Inn2flix that charged £50/month for access to just 10 B-movies, tricking victims through QR code parking scams and fake iPhone giveaways
- **Shell company laundering** - Operating over 1,000 fraudulent websites through 300 different shell companies with nominee directors to hide true ownership and evade law enforcement
- **Bypass after regulatory bans** - When German regulators banned 450 high-risk merchants from Payone, over 400 were simply moved to other Worldline subsidiaries to continue operating illegally
- **Fake virus software scams** - Indian telemarketers using fake virus pop-ups to panic consumers into buying "dubious software" and technical support services that didn't exist
- **QR code "quishing" schemes** - Placing fake QR codes on UK parking meters that directed victims to fraudulent payment sites, generating £3.5 million in losses across 800+ cases

- **Adult content subscription traps** - Dating and pornography sites with automatic renewals, hidden fees, and deceptive checkout processes designed to extract ongoing payments from victims
- **High-velocity transaction spikes** - Sudden massive increases in transaction volume that should have triggered fraud alerts but were instead facilitated through "load balancing" to hide the suspicious activity from card networks
- **Load Balancing** – adding legitimate transactions to lower the fraud rate so that merchants would not exceed Visa's acceptable level.

Worldline Denies It

Beyond the single-day 41% stock crash, Worldline shares have lost over 90% of their value since their 2021 peak.

For their part, Worldline vehemently denies the allegations. CEO Pierre-Antoine Vacheron dismissed the new allegations as an "attack" by media outlets, claiming there was "nothing new" in the reports

The company emphasized its 2023 compliance review and merchant terminations while threatening legal action against the investigating journalists.

But the companies' recent actions tell a different story. Worldline acknowledged conducting a "thorough review" of its high-brand-risk portfolio and terminating relationships worth €130 million in annual revenue.

The company also says its fraud ratio is "below the industry average," but some doubt these claims based on the "division shuffling" schemes which call into question any of their statistics and some of the load balancing activity that was mentioned during the investigation.