Merchant Scams: Fraud Hidden in Plain Sight

How fake sellers and fraudulent merchants drain businesses and consumers

Merchant scams exploit the growing trust in digital commerce. Fake sellers, fraudulent invoices, and ghost businesses cost organizations and consumers billions every year. This whitepaper explains how merchant fraud works, who is targeted, and how WeVerify's verification platform closes the gap between trust and truth.

Introduction: Commerce Is Only Safe When Merchants Are Real

Every commercial transaction starts with a basic assumption: that the seller is who they say they are, that the goods or services are real, and that the money will go where it is supposed to. Merchant scams attack all three of these assumptions simultaneously.

From fake online shops selling products that never arrive, to sophisticated invoice fraud operations that redirect payments from real suppliers, merchant scams have evolved into a major commercial and financial threat. The rise of e-commerce, digital invoicing, and marketplace platforms has given fraudsters an enormous attack surface.

This whitepaper is intended for businesses, procurement teams, marketplace operators, payment processors, and compliance professionals who need to understand how merchant fraud works and what can be done to stop it. WeVerify provides the identity verification and KYB tools that make this possible.

$48B	**1 in 5**	**72%**
global e-commerce fraud in 2023	SMEs report recurring invoice fraud	marketplace fraud involves unverified sellers

1. Types of Merchant Scams

Merchant scams take many forms, but all share a common foundation: a fraudster presenting themselves as a legitimate seller or business partner to steal money, goods, or data. Understanding each variant is the first step toward effective defense.

1.1. Fake Online Storefronts

Fraudsters build convincing e-commerce websites selling high-demand goods at attractive prices. These sites feature professional design, fake reviews, and copied product images. Payment is processed upfront. No product is ever delivered. The site disappears within days or weeks. Consumers and businesses ordering in bulk are both targets.

1.2. Invoice and Payment Fraud

Also known as Business Email Compromise (BEC), this type of fraud involves intercepting or spoofing legitimate supplier communications to redirect payments to fraudster-controlled accounts. The fraudster either impersonates the supplier directly or hacks an email account to alter banking details on real invoices. Many organizations pay before realizing the change.

SCALE OF IMPACT

The FBI's Internet Crime Complaint Center reported over $2.9 billion in BEC losses in 2023. A single successful attack on a mid-size company can redirect months of supplier payments before anyone notices. Document verification at invoice receipt would stop most of these cases.

1.3. Ghost Businesses and Shell Companies

Ghost businesses are registered legal entities with no real operations. They exist on paper to receive payments, open bank accounts, or satisfy procurement requirements. Shell companies serve a similar function, often layered through multiple jurisdictions to obscure ownership. These entities appear legitimate in basic checks but dissolve after receiving payment.

1.4. Marketplace Seller Fraud

On platforms like Amazon, eBay, or industry-specific B2B marketplaces, fraudulent sellers create accounts, build brief positive track records with cheap items, then execute large-scale fraud by taking orders and payments without fulfilling them. They use stolen or synthetic identities and business documents to register, making them difficult to trace.

1.5. Subscription and Advance-Fee Fraud

Fraudulent merchants offer services requiring upfront payment or subscription commitment. Once payment is collected, the service is never delivered, support contacts go silent, and cancellation becomes impossible. Variations include fake trade directories, supplier databases, and professional certification bodies that collect fees but provide nothing of value.

2. How Fraudulent Merchants Slip Through the Cracks

Most organizations believe their procurement or onboarding processes provide adequate protection. In practice, several common gaps allow fraudulent merchants to operate undetected:

Gap	How Fraudsters Exploit It
Basic company registration checks only	Ghost companies are registered entities; registration alone proves nothing
No verification of beneficial ownership	Shell company chains hide the real actor behind multiple layers
Manual document review	Forged documents pass human inspection; AI-detected fakes do not
No ongoing monitoring after onboarding	Legitimate sellers turn fraudulent after initial verification
Trusting email for payment instructions	BEC attacks succeed when bank details are not independently verified
No verified identity on seller accounts	Synthetic identities and stolen IDs register freely

3. The Real Cost of Merchant Fraud

The financial cost of merchant fraud is obvious. But the full impact extends well beyond direct monetary loss:

Cost Categories of Merchant Fraud

- Direct financial loss from payments made to fraudulent merchants or accounts.
- Supply chain disruption when legitimate suppliers are not paid and deliveries stop.
- Reputational damage to businesses that unknowingly transact with fraudulent entities.
- Regulatory penalties where compliance failures allowed fraudulent KYB to pass.
- Internal investigation costs and legal fees for recovery attempts.
- Customer trust damage when consumer-facing platforms host fraudulent sellers.
- Time and productivity loss across procurement, finance, and legal teams.

For small and medium businesses, a single successful merchant scam can be existential. For large enterprises, repeated exposure without systemic controls signals process failure that regulators take seriously.

4. Vulnerability Assessment: Where Is Your Exposure ?

Organizational Vulnerability Checklist

- Your organization onboards suppliers or vendors using self-submitted documents without independent verification.
- Payment details from existing suppliers can be changed via email without a secondary verification process.
- Your marketplace or platform allows sellers to register without verified identity or business documentation.
- You have no process to verify beneficial ownership of companies you transact with.
- Invoice approval does not include a check of the payee's verified bank account details.
- There is no ongoing monitoring of active merchant relationships for changes in business status.
- Fraud alerts from customers or employees do not trigger systematic account review processes.
- Your KYB process relies on public registries alone, without checking document authenticity.

5. The WeVerify Defense Framework

WeVerify closes the verification gaps that merchant fraudsters rely on. Our platform combines KYC, KYB, document authentication, and audit trails into one unified solution that works across procurement, onboarding, and payment workflows.

1. **Know Your Business (KYB) Verification**

   WeVerify's KYB checks verify business entities against official registries, validate documents like incorporation certificates and financial statements, and check beneficial ownership structures. Ghost companies and shell entities cannot produce authentic, verifiable documentation. Our system detects this.

2. **Document Authenticity Verification**

   Every document submitted in a merchant onboarding or procurement process can be authenticated in real time. WeVerify detects forged invoices, manipulated PDF files, altered bank statements, and cloned registration documents using AI-powered forensic analysis.

3. **KYC on Key Business Contacts**

   Fraudulent merchants rely on anonymity. WeVerify's individual KYC, powered by NFC identity reading and selfie matching, verifies the real person behind the business account. When the individual behind a supplier is verified, the risk of ghost merchant fraud drops dramatically.

4. **Secure Payment and Invoice Verification Workflows**

   Changes to payment details are a primary BEC attack vector. WeVerify enables organizations to require verified digital signatures and tamper-evident seals on any invoice or payment instruction. Unsigned or unverified changes are automatically flagged.

5. **Ongoing Monitoring and Audit Trails**

   Merchant verification is not a one-time event. WeVerify's platform supports continuous monitoring of verified business relationships, with instant alerts on changes to registration status, ownership, or compliance standing. All records are stored in audit-ready logs.

6. **Marketplace and Platform API Integration**

   For platforms hosting third-party sellers, WeVerify integrates directly into seller onboarding flows via API, ensuring every seller account is linked to a verified individual and business entity before they can list or transact.

Conclusion and Call to Action

Merchant fraud is a structural problem in digital commerce. As long as it is easier to fake a business than to start a real one, fraudsters will continue to exploit that gap. The answer is not more suspicion. It is better verification.

WeVerify gives organizations the tools to verify businesses and individuals at the speed of commerce, without sacrificing thoroughness or compliance. Our platform is built for the reality of modern procurement, onboarding, and marketplace operations, where speed and trust must coexist.

Every merchant you onboard without verification is a risk you have chosen to carry. WeVerify makes verification fast, affordable, and legally defensible. Start today.

Give Your Users the Protection They Deserve

WeVerify's KYB and KYC platform gives you full visibility into who you are doing business with.

Protect your supply chain, your payments, and your reputation. Register today with EUR 50 in free verification credits

www.weverify.com

Get started with EUR 50 free credit. No subscription required