

Supplier bank data verification: protecting procurement against payment misuse

Supplier bank data verification is a control process in which the procurement and finance departments verify suppliers' bank details before payments are made. Its aim is to detect false or manipulated bank data before payments are triggered. It is a central building block against payment diversion fraud, identity theft and invoice manipulation and is one of the mandatory disciplines of professional supplier master data management.

As of October 2026 · amplifa-marketplace.ai/en/glossary/lieferantenbankdatenpruefung

Key facts at a glance

- 01 Supplier bank data verification verifies suppliers' bank details before payments are approved.
- 02 Typical checks include matching the IBAN against supplier master data, a call-back to a known contact person and a plausibility-based four-eyes approval.
- 03 Common attack patterns are fake invoices, altered IBANs on genuine invoices and social engineering e-mails demanding urgent payment changes.
- 04 In practice, a documented approval process with stored verification evidence for every bank detail change has proven its worth.
- 05 As a rule, bank data should be revalidated on new supplier setup, on every change and periodically – e.g. annually.
- 06 The check protects not only against fraud but also against mispostings, returned direct debits and delayed payments to genuine suppliers.

Definition: supplier bank data verification

Supplier bank data verification comprises all measures to verify a supplier's bank details before payments are made to them. It forms part of supplier master data management and of the internal control systems against economically motivated criminal attacks.

Distinction from credit assessment

Bank data verification establishes whether the stored bank connection actually belongs to the supplier. Credit assessment, by contrast, evaluates a supplier's ability to pay and creditworthiness, e.g. via business information providers, ratings or payment ratios. The two processes complement each other: while credit assessment addresses default risk, bank data verification protects against payments to third parties. Both belong in the onboarding process and should be combined with periodic revalidation.

Legal and organisational classification

Bank data constitutes personal data as soon as it relates to a natural person – e.g. an owner or managing director. Its handling is therefore subject to GDPR principles such as data minimisation and purpose limitation. From a compliance perspective, bank data verification forms part of an adequate internal control system; auditors and bodies with liability exposure expect traceable processes. The specific design should be agreed legally on a case-by-case basis – e.g. with data protection officers and auditors.

Methods and procedure for bank data verification

Proven processes combine several levels of verification, since no single method is reliable on its own. The more sensitive the payment process, the deeper the verification should be.

Document and data checks

In the first step, the submitted bank data is checked for formal and logical consistency: Is the IBAN check digit correct? Does the bank sort code match the country and the IBAN structure? Do the beneficiary name and legal form match the master data and the invoice? Red flags include discrepant countries of registered office, private account patterns or foreign accounts held by locally based suppliers. The overall data quality of the master data – from addresses to tax numbers – is also relevant here; weaknesses flow into the data quality report of master data management.

Call-back and independent communication channel

The strongest verification step is the call-back to the supplier via an already known, independent channel – for example the stored landline number of a long-standing contact, not the telephone number or e-mail address contained in the change request itself. During the call-back, details should be clarified that only the genuine supplier would know. When dealing with unknown suppliers, an additional proof of identity is recommended, such as an official register extract or a confirmation from the supplier's bank.

Test payment and approval process

Before the first payment to a new bank connection, a small-amount test payment has proven effective in practice, the receipt of which the supplier must confirm. Alternatively, both parties confirm the account details in writing with counter-signature. Approval then follows the four-eyes principle: one role enters the data, a second – ideally from the finance department – checks and approves. Every bank

detail change is documented in the master record with verification evidence, verification date and verifier.

Key KPIs of supplier bank data verification

The verification stage can be steered with just a few key figures. These are also suitable for the data quality report and internal control reporting.

Verification rate and check rate

The verification rate indicates how many active suppliers have a verified and documented bank connection. In mature organisations, this figure typically lies close to 100 per cent for payment-active suppliers; legacy backlogs are often only covered after step-by-step revalidation. The check rate complements this: what percentage of bank detail changes went through the complete verification process?

Lead time and detection rate

Lead time measures how long a change request takes until approval. Short turnaround is important so as not to frustrate suppliers – but not at the expense of four-eyes control. The detection rate counts rejected or suspicious requests; it shows whether the process actually filters out fraud attempts. A permanently 'empty' detection rate may also mean that attacks are slipping through undetected.

Cost of verification versus loss prevention

In practice, the effort per check is often in the low double-digit euro range when standard routines and call-back scripts are used. This is set against typical losses from payment diversion fraud, which often run into five or six figures per case and are not always fully recoverable in law. This ratio justifies the check economically – even for suppliers with small volumes, since fraudsters specifically test small, inconspicuous suppliers.

Risks, fraud patterns and controls

The most important attacks on payment processes exploit precisely the interface that bank data verification secures. Buyers and finance teams should know these patterns.

Typical fraud patterns

In CEO fraud, perpetrators pose as senior management and demand urgent payments or account changes. In the fake supplier scam, a completely fictitious supplier is set up with plausible documents. In invoice swapping, only the IBAN on a genuine, copied invoice is altered – often shortly before the payment due date to create time pressure. Social engineering via e-mail from compromised supplier mailboxes is also widespread. Projects with close just-in-time relationships and a high payment frequency are particularly vulnerable, as short response times are expected there.

Organisational controls

Key controls are: segregation of master data maintenance and payment approval, the four-eyes principle for every bank detail change, no changes on the basis of an e-mail instruction alone, system permissions on a least-privilege basis, and protecting supplier portals with two-factor authentication. In addition, standard queries in the ERP should check whether a new IBAN already appears for other suppliers, employees or in fraud databases. Duplicate checks and rules for country and currency patterns complete the net.

Collaborative prevention with the supplier

Prevention works best jointly with the supplier: agree binding change processes, named contacts and documented channels for bank detail changes in contract management. Raise suppliers' awareness of fake e-mails 'in the name of your buyer' and stipulate that payment changes are never instructed via ordinary e-mail threads. Internal awareness-raising among procurement, accounts payable and controlling is also part of this – fraudsters deliberately target the weakest link in communication.

Process sequence: from onboarding to the payment run

Bank data verification is not an isolated step but a segment within the payment process, from supplier setup to the payment run. Cleanly defining the interfaces avoids friction losses.

Onboarding and master data setup

During onboarding, bank data is captured together with the commercial register extract, tax data and, where applicable, certificates. The verification should be integrated into the standard workflow for disposition and master data maintenance, similar to how disposition parameter maintenance defines defined fields and rules for day-to-day operations. Only after verification is complete is the supplier released for orders and payments. Change requests go through the same channel with the same level of verification.

Before the payment run

Immediately before the payment run, a final check takes effect: for changes younger than a defined threshold – in practice usually 30 to 90 days – the payment is blocked or subjected to special approval. New IBANs on invoices with a high amount or short payment terms trigger a manual call-back. This combination of dwell-time control and amount/deadline heuristics catches most late-arriving manipulation attempts without slowing down normal operations.

Periodic revalidation

Even unchanged bank data ages: accounts are closed, suppliers change banks. Periodic revalidation – in practice usually annually or biennially, tiered by supplier volume – keeps the master data up to date. Revalidation can be readily embedded in the routine supplier review, together with certificate status, credit assessment and terms updates. Anyone who is anyway negotiating early payment discounts or payment days can request the account confirmation at the same time and save process costs.

Current developments and digital tools

Payment diversion fraud is becoming more professional – but verification technology is also evolving. Procurement and finance teams should know the state of the art without becoming dependent on individual tools.

Automated IBAN validation and data matching

Modern systems automatically check IBAN structure, check digit, sort code assignment and registry data as soon as data is captured. In addition, data matching can be run against registers, fraud databases and internal blacklists. Such automation reduces the routine error rate and relieves verifiers, but does not replace the call-back: human confirmation via an independent channel remains the core of the verification. AI-supported anomaly detection on payment flows is also increasingly widespread, but should be understood as an additional signal rather than the sole basis for decisions.

Standardised supplier portals

More and more companies only permit bank detail changes via an authenticated supplier portal with two-factor authentication. This significantly reduces e-mail-based attacks and automatically creates an audit-proof verification trail. For suppliers without portal access, a form-based process with original submission and call-back remains. Standardisation also helps when onboarding new suppliers, for example within a category playbook or a supplier shortlist, where process orientation should be considered from the outset.

What remains manual and critical

Despite automation, two points remain manual: the assessment of the economic legitimacy behind an account change, and the person-to-person call-back. The interface to negotiation management also remains critical: changes to account details, invoice addresses or payment routes should never be communicated 'on the side' within ongoing price or negotiation processes. Fraudsters deliberately exploit such situations, because vigilance drops there and many parties are communicating simultaneously.

Typical metrics

Metric	Typical value
Verification rate of active suppliers	typically > 98 % <i>Proportion of payment-active suppliers with a documented, verified bank connection</i>
Check rate for bank detail changes	100 % <i>Every change must go through the full verification process; exceptions are documented</i>

Lead time for bank detail changes	typically < 5 working days <i>Time from receipt of request to approval, incl. call-back</i>
--	--

Detection rate	documented > 0 <i>Number of rejected/suspicious requests per year; a sustained zero may indicate undetected cases</i>
-----------------------	--

Practical example

A medium-sized mechanical engineering company with around 1,200 active suppliers received an e-mail shortly before Christmas from a long-standing sheet metal supplier: new bank details, payment due date in three days. The procurement officer handling the request almost complied – but the call-back via the stored landline number revealed that the supplier had made no change to its account. The incident led to a revised process.

- Bank detail changes only via the supplier portal or a signed original form, with a call-back to a known contact person
- Systematic blocking logic: payments to IBANs changed less than 30 days ago require a second approval from the finance department
- Annual revalidation of all payment-active suppliers, embedded in the existing supplier review
- Awareness training for procurement and accounts payable with real attack case examples, twice a year

Conclusion

Supplier bank data verification is a comparatively low-cost control mechanism with a high loss-prevention effect. It is only effective as a combination of formal checks, independent call-back, four-eyes approval and documented evidence. Anyone who regulates change channels bindingly in contract management and integrates verification into onboarding as well as the payment run removes the most common attack surfaces. Periodic revalidation and a few clear KPIs keep the process stable over time. For buyers and supply chain managers, it is therefore part of the basic hygiene of supplier management – not an optional extra.

Frequently asked questions

? How do I check a supplier's bank details?

First check the IBAN for formal correctness and consistency with the master data. Then verify the change via a call-back using an independently held contact route and, where necessary, request an commercial register extract or a confirmation from the supplier's bank. Payment should only be made after documented approval under the four-eyes principle.

? **How can I recognise a fraudulent supplier invoice with a changed IBAN?**

Warning signs include short-notice changes immediately before the payment due date, new IBANs with a different country pattern, changed contact persons and pressure for urgency in the request. Always compare the IBAN with the master data, not just with earlier invoices – fraudulent invoices frequently copy genuine ones. If in doubt: call back rather than pay.

? **Who is responsible for supplier bank data verification – procurement or accounts payable?**

In practice, master data maintenance often sits with procurement or the shared service centre, while payment approval rests with the finance department. What matters is the segregation of roles: whoever enters bank details must not approve them alone. Responsibilities should ideally be defined in writing in the process document, with defined thresholds and escalation routes.

? **How often should supplier bank data be revalidated?**

It is common practice to periodically revalidate all payment-active suppliers at intervals of one to two years, tiered by payment volume and risk profile. For sensitive suppliers or after incidents, a shorter interval may be sensible. Importantly, revalidation should apply the same depth of checks as the initial onboarding.

? **What does a supplier bank data verification cost?**

With standardised processes, the effort typically lies in the low double-digit euro range per check, possibly slightly higher without automated tools. This is set against losses from payment diversion fraud, which frequently run into five or six figures per case and are not always recoverable. Economically, the check therefore almost always pays off.

? **May I request a commercial register extract or bank confirmations as part of the bank data verification?**

Yes, such evidence is a standard means of identity verification and is usually accepted by reputable suppliers. However, observe data protection principles: only collect data that is necessary for the payment purpose. The specific design and any industry-specific requirements should be reviewed legally on a case-by-case basis.

Find the right suppliers on Amplifa

Verified industrial suppliers in Germany, Austria and Switzerland. Describe your requirement and receive comparable offers.

amplifa-marketplace.ai