CIPFA The Chartered Institute of Public Finance & Accountancy

protecting your supply chain from fraud

In times of emergency there is a need to respond quickly but to also ensure continued vigilance against the risks of fraud, bribery and corruption. The information below acts as a reminder of the continuing risks to supply chains posed by fraud and corruption, many of which are exacerbated by emergency circumstances.

Key points:

- **If something looks too good to be true it probably is!**
- **Make sure that you document all decisions**
- **Not everything needs to be procured urgently – don't be pressurised**

Don't forget the good habits you already have

Local Government Association

CIPFA COUNTER FRAUD CENTRE

What to look out for	How to protect your organisation
Remain alert to risks of **mandate fraud**. Fraudsters purport to be from a supplier and request a change to a direct debit, standing order or bank account details to divert payments to themselves.	On receiving a request to change bank details: ■ Contact the approved person at the supplier as recorded on your finance system. ■ Use the contact details on finance system. ■ Do not reply to the email you were sent, use the email on the finance system. ■ Use the phone number on the system, not on the invoice or email received.
Guard against **fictious and unqualified suppliers** by continuing **due diligence** on new suppliers.	Prior to approving a new supplier: ■ Obtain Companies House verification. ■ Perform VAT registration checks. ■ Ensure bank details and registered office are independently verified.
Remain alert to collusion and cartel activity including: ■ market sharing ■ bid suppression ■ price fixing ■ provision of fraudulent information. In emergencies increased demand and accelerated timescales increase risk.	To guard against collusion: ■ Include declarations of non-collusion in tender docs. ■ Monitor which suppliers win tenders. ■ Ensure fraud reporting mechanisms are in place and publicise these to the supplier. ■ Ensure that you document all decisions.
Do not forget about conflicts of interest: especially important given the likely increased use of single sourcing and direct awards.	To manage the impact of conflicts of interest: ■ No one person should be responsible for procurement decisions. ■ Document all decisions. ■ Use conflict of interest registers to check known connections.
Purchasing goods, works or services that are not required can be motivated by a **personal connection** to the supplier or in exchange for **kickbacks**.	Look out for: ■ Bids tailored to certain suppliers. ■ Close relationships between staff and suppliers. ■ Ask suppliers to provide conflicts of interest information. ■ Check internal conflict of interest registers.
Contract splitting to avoid additional scrutiny can also be motivated by a **personal connection** to the supplier or in exchange for **kickbacks**.	To identify contract splitting/links to suppliers: ■ Monitor spend with suppliers. ■ Ask suppliers to provide conflicts of interest information. ■ Check internal conflict of interest registers.

What to look out for	How to protect your organisation
Duplicate invoices submitted by suppliers.	To identify and prevent duplicate payments: ■ Carry out spend analysis. ■ Implement 'no purchase order, no pay' policies. ■ Perform spot checks and post-implementation checks.
Inflated claims submitted by suppliers – greater risks given payment in advance, payment on order instead of receipt, and payment by results.	To identify and prevent inflated claims: ■ Carry out spend analysis. ■ Implement 'no purchase order, no pay' policies. ■ Perform spot checks and post-implementation checks when feasible.
Product substitution – low quality goods or services are provided but the charge is for a higher quality product. Could be sub-standard, used, or counterfeit products. This is a greater risk in an emergency given stretched resources and higher volume procurement.	To identify and prevent product substitution: ■ Implement 'no purchase order, no pay' policies. ■ Perform spot checks and post-implementation checks when feasible. ■ Set up quality monitoring or customer feedback mechanisms where possible.
Fraudulent progress reports submitted by suppliers. This poses a significant risk where past performance is used to determine future payments.	To guard against the submission of fraudulent information: ■ Request information from third parties to reduce reliance on supplier-generated numbers/assurances. ■ Carry out spot checks when feasible. ■ Request supporting evidence.
Misappropriation of assets through delivering to a home address or fictitious address – by staff or suppliers. Higher risk with many people working remotely and increased levels of procurement by new suppliers.	To guard against asset misappropriation: ■ Notify suppliers of approved delivery addresses. ■ Use inventory and asset registers. ■ Monitor usage where feasible. ■ Monitor purchase card spend. ■ Monitor delivery addresses. ■ Monitor use of third-party online shopping platforms.

What can you do to protect your organisation?

- Continue to raise awareness of fraud, bribery and corruption risks with your staff, suppliers and contractors – including when onboarding new starters and volunteers.
- Make a clear statement of 'zero tolerance' of fraud, bribery and corruption and include details of your fraud reporting mechanism in contracts and communications.
- Continue to conduct due diligence on new suppliers and contractors – including checking against the bank accounts of staff and existing suppliers for any matches, which could indicate payment diversion or fictitious suppliers.
- Continue to conduct due diligence on staff, contractors and volunteers – including verifying any necessary qualifications and that police checks are in place and up to date.
- Implement a robust verification process for bank account change requests, to protect your organisation from mandate fraud and fictious suppliers used for payment diversion.
- Champion compliance through 'no purchase order, no pay' policies, supplier due diligence and up-to-date contract procedure rules.
- Use analysis of spend data to identify off-contract spend or duplicate invoices and monitor aggregate spend for contract splitting.
- Monitor purchase card spend – consider the additional risks as people work remotely, with reduced oversight.
- Continue to keep up-to-date inventory and asset registers and monitor usage levels where possible.
- Support the use and management of conflicts of interest policies and procedures, including registers.
- Make use of open book accounting and right to audit clauses where possible.

CIPFA The Chartered Institute of Public Finance & Accountancy

Registered office: 77 Mansell Street, London E1 8AN
T: 020 7543 5600 F: 020 7543 5700 www.cipfa.org

The Chartered Institute of Public Finance and Accountancy, registered with the Charity Commissioners of England and Wales No. 231060 and the Office of the Scottish Charity Regulator No.SCO37963. CIPFA Business Limited, the trading arm of CIPFA that provides a range of services to public sector clients, registered in England and Wales no.2376684.

04/2020