



COVID-19 FRAUD RISKS

Alert: March 2020

The World Health Organization (WHO) labelled COVID-19 a “global pandemic” and, sadly, this brings with it an increased risk of fraud across all sectors.

With organisations facing many different pressures during a crisis, fraudsters look to exploit the lapses and changes in controls to gain financially. This document highlights some of those risks with accompanying advice on mitigation.

Risk area	Contributing factors	Mitigation
Cyber fraud The rise in online communication can heighten vulnerability to cyber, data security, and privacy threats. Cyber criminals will actively look to exploit these threats.	<ul style="list-style-type: none"> • Phishing emails exploiting Covid–19 • Staff working outside of any secure network • Sensitive data being transferred between insecure environments 	<ul style="list-style-type: none"> • Staff should follow the principles set out in our Covid-19 email scams guidance document • Staff should ensure communications are encrypted / password protected if sending outside of the secure network • IT functions should disseminate guidance about remote working
Misappropriation Urgency to obtain equipment results in greater volume of assets available to be misappropriated, and the severity of the threat may result in staff stockpiling	<ul style="list-style-type: none"> • Controls may be relaxed to allow prompt movement of supplies between sites and organisations • Black market value equipment and consumables incentivises individuals to steal 	<ul style="list-style-type: none"> • Stock records and asset registers should be maintained as far as possible, with audit trails of urgent activity retained • Exception reporting should be utilised frequently • Concerns should be raised immediately
Supplier interaction A higher demand and desire to procure equipment quickly can lead to a lapse in compliance with procurement processes	<ul style="list-style-type: none"> • Urgency to procure goods and services reduces time to complete adequate due diligence • Shortage of supply may require organisations to engage with different and off framework suppliers • Controls around tender waiver and contract extension activity may be relaxed 	<ul style="list-style-type: none"> • Due diligence should be pursued to the greatest extent in the time frame available, with checks continuing to progress to completion even post procurement • Provision should be allowed for retrospective challenge and cost recoveries • Cumulative supplier spend should be monitored regularly

Risk area	Contributing factors	Mitigation
Accommodation Additional and often high cost accommodation may be required for key staff that need to remain away from their usual address due to others self-isolating	<ul style="list-style-type: none"> Hotels may exploit the crisis by overcharging room rates or incidentals Staff may exceed the permitted allowances in meal / incidental charges 	<ul style="list-style-type: none"> Accommodation should be booked centrally using arranged rates Charges over and above an agreed threshold for subsistence should be agreed with the hotel that they will be paid by the employee and reclaimed through expenses
Invoice fraud Accounts payable processes will be streamlined to ensure prompt and advance payments for urgently required goods and services	<ul style="list-style-type: none"> Urgent payment requests exploiting Covid – 19 Relaxed segregation and authorisation processes may allow false or inflated invoices to be paid Mandate change requests cannot be easily verified as suppliers are under pressure and key contacts may be working remotely Government advice to maintain supplier payments irrespective of performance 	<ul style="list-style-type: none"> Staff should follow the principles set out in our Covid-19 email scams guidance document Invoices should be carefully confirmed against orders and rates agreed specifically in the crisis Goods receipt should be confirmed prior to payment Supplier change requests must be confirmed using verified contact information Queries to be resolved retrospectively must be logged for follow-up
Credit cards Departments may rely more heavily on credit cards to promptly secure locally required goods, and inappropriate purchases may not be able to identified	<ul style="list-style-type: none"> Credit card expenditure is anticipated to temporarily increase during this period Cards are likely to be used by multiple individuals due to increasing pressure Expenditure is reviewed retrospectively Non-essential or inappropriate purchases may not be able to be promptly identified or attributed to an individual 	<ul style="list-style-type: none"> Records of card whereabouts should be maintained wherever possible Itemised receipts should be retained for all credit card purchases Statements should be reviewed and challenged promptly
Expenses An anticipated increase in travel and subsistence expenses as a result of staff working additional hours and across various sites may obfuscate fraudulent claims	<ul style="list-style-type: none"> Expenses claims may be subject to limited verification in the interest of prompt payment Expenses may be incurred for remote working equipment Claims may be made for expenses not incurred Claims for subsistence may exceed daily allowances 	<ul style="list-style-type: none"> Evidence of original expenditure should be required Guidance, updated as necessary to reflect changes to allowances and process during Covid-19, should be issued to staff

Risk area	Contributing factors	Mitigation
Governance As audit committees and board meetings are suspended there may be limited reporting and oversight across operations	<ul style="list-style-type: none"> • Less frequent meetings or business critical focussed meetings may result in a period without scrutiny of financial and other decision • Staff and management may be acting with more autonomy in undertaking financial functions 	<ul style="list-style-type: none"> • Wherever possible, virtual meetings should continue • Interim financial reports should be shared with members to ensure oversight remains in place • Changes to streamline control environments should be reported to members so that appropriate assurance measures can be considered
Payroll Payroll processes will be streamlined to ensure prompt payment, increases in workforce may obfuscate payroll fraud and complex change and reimbursement arrangements may result in salary overpayments	<ul style="list-style-type: none"> • Ghost employees may be entered onto the system • Temporary staff that are added to the payroll may remain on the system post Covid-19 	<ul style="list-style-type: none"> • Backing data should be reviewed to confirm new employees being entered onto payroll are genuine • Segregation of duties should be maintained as far as possible • Management information should be reviewed regularly to identify multiple payroll records being paid into the same bank account • Payroll records created during Covid-19 should be reviewed periodically
Recruitment An increase in staffing demand due to self-isolation and increasing pressures will prevent the application of some existing pre-employment screening processes	<ul style="list-style-type: none"> • New applicants without the appropriate qualifications or right to work status, or with criminal records, will seek to exploit the opportunity to commence employment whilst screening is pending • Staff in training and former staff not currently regulated may be able to join or return to the workforce • Safely onboarding specialist staff whilst maintaining social distance will be challenging • Advanced Disclosure and Barring Service (DBS) checks may not be available 	<ul style="list-style-type: none"> • Pre-employment screening should be pursued to the greatest extent in the time frame available, with checks continuing to progress to completion even post recruitment • In lieu of DBS confirmation, decisions to proceed should be risk assessed and documented. More stringent references, ideally from professional bodies, should be sought. • Document scanners should be utilised wherever possible

Risk area	Contributing factors	Mitigation
Duties not fulfilled Significant volumes of staff will be working remotely, some having done so at short notice.	<ul style="list-style-type: none"> • Certain elements of some roles may not be able to be completed remotely • Systems may not be established to monitor staff activity remotely • Some staff may inflate symptoms to secure paid self-isolation periods from their substantive employer, in order to undertake lucrative agency or other work elsewhere • Organisations will be required to accept documentation in lieu of a fitness to work certificate 	<ul style="list-style-type: none"> • Guidance should be provided to remote workers on how their workload should be managed and reported • Exception reporting should be utilised frequently • Management information should be reviewed regularly to identify staff abusing self-isolation requirements • Shielding documentation should be verified against known information
Temporary workforce Additional staff usage may be increased due to self-isolation and increasing pressures	<ul style="list-style-type: none"> • Agency staff may commence engagements whilst screening is pending • Demand will increase cost of additional staffing • In some services additional overtime may be required, and timesheets may be subject to limited verification due to pressures 	<ul style="list-style-type: none"> • Screening should be pursued to the greatest extent in the time frame available, with checks continuing to progress to completion even post engagement • Additional staff identity must be confirmed at their first shift • Invoices should be carefully confirmed against booking requests for hours and rates • Timesheets should be verified by individuals who were physically present at the time of the shift, and using local records and knowledge
False claims Significant volumes of staff will be working from home, some having done so at short notice, and staff may be recruited prior to occupational health reviews, which may result in increased claims for compensation for injury	<ul style="list-style-type: none"> • Staff may be required to work from home for a prolonged period, which may result in inflated claims for injury as a result of the use of inappropriate home workstations • Staff may be required to commence work prior to completion of an occupational health assessment, which may result in inflated claims for injury or illness • Potential exposure to Covid-19 due to limited availability of PPE may result in false claims 	<ul style="list-style-type: none"> • Guidance should be provided to remote workers to assist them with the set up of home workstations • Occupational health assessments should be pursued as promptly as possible in the circumstances • Adequate audit trails of PPE whereabouts and availability should be maintained as far as possible

The Counter Fraud team at RSM is closely monitoring the fraud risk developments across the sector and beyond to highlight areas of concern as well as best practice. The team will continue to provide guidance to ensure that organisations can remain astute to the risks.

In the meantime, staff should follow these key principles:

Report any frauds promptly

All concerns of fraud, bribery and corruption should be reported promptly to your manager, the finance team and Internal Audit. Staff should not be concerned that they may be wrong, or that this will create unnecessary delay.

Be alert for fraudulent cyber communications

Unfortunately, we have already seen an increase in attempted phishing attacks using Covid-19 information as click bait. Follow the principles set out in our Covid-19 email scams guidance document, and if in doubt, contact your IT support immediately.

Finance fraud

Seek to verify invoices, requests for payment and changes to supplier bank account information as far as you are able to in the circumstances. Seek procurement advice when engaging with a potentially new supplier, liaise with colleagues to confirm receipt of goods and check you know who you are corresponding with.

Timesheet fraud

Confirm timesheets and claims prior to authorisation by liaising with colleagues who were physically present at the time of the shift and using local records and knowledge. A small investment of time here will ensure your budgets are not impacted by fraudulent claims when staffing levels are critical.

Emerging risks

As the crisis develops new risks will present themselves and whilst it is not possible at the moment to fully gauge these, it would be worthwhile considering the impact they may pose:

Furlough working

The government have committed to cover 80% of salaries so that companies do not need to make staff redundant during this period. Individuals are not permitted to undertake other work during this period, however it is not currently clear if overpayments as a result of staff who abuse this benefit could be recovered from the organisation.

Remote working

It is likely workloads will reduce should remote working requirements exist for sometime. Organisations should ensure that staff are aware of what is expected of them, and identify additional work or projects that can be undertaken to keep staff occupied, with appropriate and regular management monitoring and oversight. Any future investigations of staff dishonestly failing to complete their working hours may be hampered were expectations not expressly communicated.

For further information please contact

Tim Merritt

Head of Fraud Risk Services

07768 873701

tim.merritt@rsmuk.com

Andrea Deegan

Director

LCFS

07817 002136

andrea.deegan@rsmuk.com

Gemma Higginson

Associate Director - London

LCFS

07800 718680

gemma.higginson@rsmuk.com

Erin Sims

Associate Director - London

LCFS

07800 617456

erin.sims@rsmuk.com

Matt Wilson

Managing Consultant - South

LCFS

07484 040691

matt.wilson@rsmuk.com

Bradley Vaughan

Managing Consultant - North

LCFS

07436 268331

bradley.vaughan@rsmuk.com

www.rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Employer Services Limited, RSM Northern Ireland (UK) Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Before accepting an engagement, contact with the existing accountant will be made to request information on any matters of which, in the existing accountant's opinion, the firm needs to be aware before deciding whether to accept the engagement.