KANTAR

Fraud Reporting

7 MINUTE READ

Our policy on...
Fraud Reporting

First issued: November 2021

Last updated: June 2024

The way we work makes all the difference

As you know, business integrity is the cornerstone of who we are and what we stand for here at Kantar.

It's part of our DNA and how we operate.

Like all large and complex companies, we're exposed to a broad range of internal and external fraud risks, and this policy outlines the role that you can play in helping us to prevent, detect, combat and report all forms of fraud.

Our zero-tolerance approach to fraud extends to all applicable laws/regulations in every country we operate. That means we'll investigate all potential, attempted and actual frauds (no matter how small), reporting to external law enforcement as necessary, with potential liability for civil and criminal penalties alongside internal disciplinary action, including termination of employment.

For clarity, this policy applies to all Kantar colleagues globally, including directors, officers and employees, as well as third party agents, consultants and intermediaries acting on Kantar's behalf.

Please read this policy carefully to understand your key role in our response to the risk of fraud within Kantar. It provides you with guidance on how to identify fraud, what to do if you discover or suspect that a fraud or attempted fraud has taken place, and the reporting mechanisms we've implemented.

Any breach of this policy may result in disciplinary action being taken including, in serious cases, potential dismissal or termination of a contingent worker's engagement. This policy is not part of your employment contract or contract for services and Kantar can change or update it from time to time.

01 What is Fraud?

Fraud includes any dishonest act, omission or representation which is intended to result in financial or personal gain, or to cause loss to another party.

A fraud can include acts such as deception, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts, and collusion. It can often accompany other issues, such as bribery/corruption, money laundering, tax evasion, anti-competitive behaviour and sanctions violations.

02
Common types of fraud to look out for

Invoice fraud

The use of false invoices or payment details is a common form of fraud faced by our business.

In broad terms, this type of fraud can be directed against Kantar itself or our customers, as follows:

- A fraudster may claim to be one of our legitimate suppliers and ask for a genuine invoice to be paid to a different bank account under the fraudster's control
- A fraudster may deceive a Kantar customer by claiming to be a Kantar business and requesting that payment for one of our invoices is redirected to one of their accounts instead
- Internal and external parties may use false, duplicate or inflated invoices, which often include vague or incomplete information regarding the goods or services provided, to defraud Kantar for personal gain

Phishing emails and "urgent payment" fraud

Phishing emails (fraudulent emails disguised as legitimate communications and designed to deceive the recipient into providing confidential information, such as passwords or financial details) are increasingly common. For instance, Kantar has experienced phishing emails in which the fraudster claims to be a senior Kantar executive and asks a colleague to make an urgent payment to a specified bank account under the fraudster's control. Contact may also be made by way of a telephone call from the fraudster directly to a colleague involved in the payments process, also known as "vishing".

Expenses fraud

A colleague dishonestly makes a claim for personal expenses rather than legitimate business expenses, or claims for the same expenses more than once.

Incentives fraud

A colleague or respondent uses market research incentives for personal gain e.g. where researchers falsify responses and take incentives for personal gain, respondents attempt multiple responses to game the incentive system, internal or external people gain access to a respondent's accounts and amend the details to personally gain from their incentives, or colleagues steal incentives.

03 How to prevent and report fraud

If you suspect any form of actual or attempted fraud, irregularity, impropriety or an information security incident, you must report it as soon as possible in accordance with this policy. This is vital to limiting damage to the organisation, preserving evidence that can assist investigations, and helping prevent future frauds.

We want to support you and ensure we get everything right.

What to do if you suspect fraud...

1. Let Kantar know by using the **Right to Speak** service. The team will then triage the reported issue and involve the appropriate colleagues from finance, HR, cyber and security to investigate as appropriate.

2. If you're asked, please try to comply with all requests for information from the investigating team as soon as possible

3. If, and only if, there is an immediate risk of destruction, and after obtaining the prior guidance from the investigating team, promptly secure all IT devices (e.g. laptop, phone, USB sticks, DVDs) and hard copy information away from anyone who may be suspected of being involved in the actual or potential fraud.

4. If, and only if, there is a risk of deletion or destruction of information, and after obtaining the prior guidance of the investigating team, contact the Global Cyber Security team, who will work with the system administrator to request that the user accounts for Microsoft Active Directory and any other key systems (e.g. Maconomy/Dynamics/Navision, IT Admin accounts, OneDrive, remote access, etc.) are disabled promptly, but not deleted.

5. Following the guidance of the investigating team, record the time, date and person responsible for all actions taken (e.g. impounding user devices, disabling accounts), and the names of those who have witnessed the action taking place.

6. Be aware that Kantar may be subject to legislation regulating financial crimes in countries or regions other than your own. Where appropriate, the investigating team will liaise with Legal to ensure we obtain the necessary legal advice on our risk exposure and obligations in each applicable jurisdiction.

Continued on next page

03
How to prevent and report fraud
continued ...

What to not to do if you suspect fraud...

1. Alert the person or people who you suspect might be involved in the fraud.

2. Place yourself in harm's way. If there is any possibility of personal harm, remove yourself and any others to safety before reporting your suspicions.

3. Attempt to start investigating – using computer equipment may compromise evidence.

4. Attempt to question any suspected individual(s) without prior approval from the investigating team.

5. Speculate or share any information with your colleagues, managers or team without explicit approval from the investigating team - these matters are sensitive and confidential and should only be discussed with the investigating team.

6. Discuss the matter outside of work, on social media or with members of the media.

7. Store any evidence in shared cupboards, drawers or anywhere that could allow another person an opportunity to modify or destroy any evidence.

8. Attempt to trap someone into admitting to, or participating in fraud.

9. Investigate a suspect's mailbox, shared drives, papers or other data without clear authorisation from the investigating team. To ensure that all evidence is preserved appropriately, this sort of activity will usually be undertaken by the Internal Audit team or the Global Cyber Security team rather than the person who is reporting the fraud.

04
What happens once you report a fraud issue...

By raising concerns, you're doing the right thing. All reporting of misconduct or suspected misconduct is confidential and will be carefully studied. This means your report will only be shared with a limited number of people, all under an obligation to keep the report confidential. We do not allow retaliation against anyone who has raised concerns. In fact, ANY retaliation will be misconduct and should be reported.

Once a report is received (other than through the 24-hour Kantar Right to Speak service, for which Group Legal is responsible), the Group Director of Internal Audit and Risk is responsible for alerting the appropriate Response Owner who will investigate and take appropriate action depending on the type of fraud experienced.

When we investigate an incident, we'll explore whether there are additional procedures, controls or training needed to make sure that it doesn't happen again. We will also notify Kantar's Audit Committee, which is responsible for reviewing fraud across the Kantar group.

Thanks again for the crucial role you'll play in preventing and reporting fraud across our business. Together, we can demonstrate the Kantar way of working – by behaving ethically, lawfully and with integrity.

05 How you can help...

All colleagues at Kantar must complete our online training when requested. If you're a new starter, you'll complete it within two weeks of joining.

Management must ensure they're aware of the specific risks of bribery and corruption in their business and location. The risks must be evaluated regularly, and appropriate mitigating procedures put in place and recorded in the risk register.

If any colleague encounters a situation of possible or actual bribery or corruption, they must immediately contact their local or regional management, who must seek advice from Kantar's Legal and Compliance teams. The 24-hour Kantar Right to Speak service is also available as a reporting channel.

Above all, everyone at Kantar needs to understand that bribery is illegal. We cannot promise to make, pay or receive bribes.

It's simply not our way of doing business.

06 Key contacts:

If you wish to report anonymously, please use the **Right to Speak** service.

For any questions about this policy, please contact the Group Director of Internal Audit and Risk or the Group Director of Finance.