More than a match for fraudsters

How to combat sophisticated fraudsters who use information technology, social network analysis and psychology to target payment processes

pwc

www.pwc.ch

Is your organisation ready to combat today's fraudsters?

These days, sophisticated fraudsters use information technology, social network analysis and psychology to target payment processes.

Fraud Risk and Control Framework

Understanding your organisation's readiness to combat today's fraudsters is essential. PwC's Fraud Risk and Control Framework covers fraud and corruption control holistically, splitting it into four key elements and then further into their component processes and controls. The key elements are:

- Planning and resourcing
- Prevention
- Detection
- Response.

Planning and Resourcing

- Fraud and corruption control planning
- Review of the fraud and corruption control plan
- Fraud and corruption control resources
- Internal audit activity in the control of fraud and corruption

Response

- Policies and procedures
- Investigation
- Internal reporting and escalation
- Disciplinary procedures
- External reporting
- Legal action for recovery of losses
- Review of internal controls

Prevention

- Implementing and maintaining an integrity framework
- Line management accountability
- Assessing fraud and corruption risk
- Communication and awareness
- Employment screening
- Supplier and customer vetting

Detection

- Implementing a fraud and corruption detection program
- Role of the external auditor in detection of fraud
- Avenues for reporting suspected incidents
- Whistleblower protection program

Controlling the fraud risk within your business starts with understanding fraud trends

Fraud risk assessments form a key part of a fraud risk and control framework. They concentrate on current fraud schemes and scenarios.

Our assessments aim to identify activities that can significantly impact your organisation's reputation, expose the company to criminal or civil liability, or result in a financial loss. Such a fraud risk assessment includes examining the existing systems, processes and the control environment to identify high risk transactions and the potential for misappropriation by either employees, related parties and/or third parties. The assessment evaluates whether or not processes and controls can be circumvented, including the susceptibility of controls to management override.

A fraud risk assessment differs from a typical operational business risk assessment as it is specialist in nature. An average employee is not a fraudster, and therefore cannot think like one. To identify the existing fraud risks within your business, specialist knowledge is required. We assess your business in light of our accumulated knowledge of various fraud schemes currently used in your industry.

Current fraud trends: social engineering on the rise

These days fraudsters are increasingly targeting organisations' payment processes using so-called social engineering techniques. Unlike plain hacking, social engineering is the art of manipulating people so they involuntarily give up confidential information, or act against company processes and policies. With the help of a combination of information technology, social network analysis and psychology, social engineers pass themselves off as customers, suppliers, and/or perhaps as your own company's management to trigger the transfer of funds from the business.

Example:

Transferring pension fund assets using a fake identity

A Swiss pension fund received a request to pay out the balance of a customer account because the customer was relocating abroad. After a series of email and phone conversations, including supporting documents sent by the fraudster by email, the funds were transferred to a bank account in Vietnam bearing the customer's name (but opened by the fraudster). The monies were then withdrawn in cash the same day.

Want a high return on investment? Proactive mitigation and detection of fraud

Proactive steps can be taken to protect your business investment and mitigate your risk of fraud. Sophisticated data mining techniques can uncover fraud within your business before funds become unrecoverable.

We recommend that in addition to performing a fraud risk assessment, you establish a fraud risk and control framework. This should include, but not be limited to, the following preventative and detective measures:

Fraud risk policies and procedures

Clear, unambiguous policies act as a deterrent to fraudulent behaviour, and complementary procedures will minimise the risk of fraud and theft occurring in an organisation. We help you develop these policies and procedures to ensure that your employees understand their duties and responsibilities to management with respect to fraud and theft within the organisation.

Pre-employment screening of employees

Your first line of defence in terms of fraud risk is pre-employment screening. You need substantial resources to verify an employee's identity, education, professional qualifications, employment history and references. PwC can help you screen potential employees by verifying at least the following required information:

- Education and qualification records
- Credit history and bankruptcy details
- Criminal records
- Media reports, including social network analysis

Business partner due diligence

Background verification procedures run on business partners, suppliers, customers, agents, etc., are needed to determine the reputation and integrity of the entities of interest and the individuals within these entities. In addition to the searches on individuals mentioned above, the checks should include:

- Regulatory information concerning companies and individuals
- Financial details such as bankruptcy, litigation and credit histories
- Asset ownership particulars such as property, boat and aircraft ownership
- References in the global media, including social network analysis

We use the latest software solutions to get the best out of your business partner due diligence.

Example:

CEO who got promoted despite embezzlement

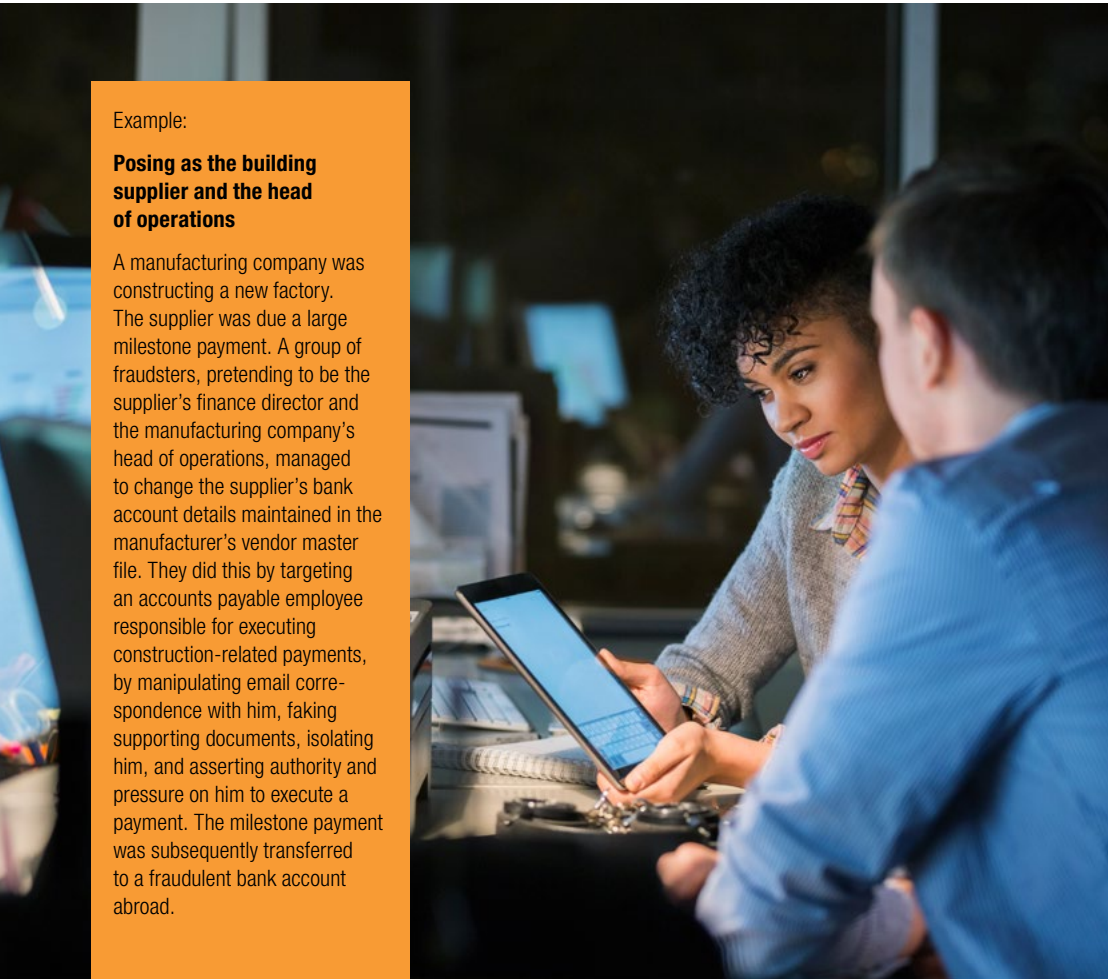
A company hired an employee who was years later promoted to a position of trust – subsidiary CEO. After laying him off, the company found out that he had defrauded his previous employer. A subsequent investigative analysis uncovered collusion with a supplier that resulted in major embezzlement of company funds.

Suspicious transaction analysis

PwC uses suspicious transaction analysis software programs to match data and interrogate an organisation's customer, supplier and employee databases to quickly identify things like duplicate payments (made either fraudulently or in error), collusion between suppliers and employees, suppliers and customers fitting known fraud profiles, and questionable transactions and payments. This automated fraud detection and data analysis process can quickly search through millions of financial transactions and master file data to identify any suspicious transactions.

Corporate investigations

If you suspect a financial loss or the theft of sensitive data you need a predetermined plan to act quickly and appropriately. Professional, experienced investigators can help you secure and gather evidence (including computer forensics), advise on communication with interested parties, quickly assess the loss, its cause, and remedy controls. We at PwC also identify loss recovery options from individual asset holdings, insurance policies or other third parties involved in the loss.



Example:

Posing as the building supplier and the head of operations

A manufacturing company was constructing a new factory. The supplier was due a large milestone payment. A group of fraudsters, pretending to be the supplier's finance director and the manufacturing company's head of operations, managed to change the supplier's bank account details maintained in the manufacturer's vendor master file. They did this by targeting an accounts payable employee responsible for executing construction-related payments, by manipulating email correspondence with him, faking supporting documents, isolating him, and asserting authority and pressure on him to execute a payment. The milestone payment was subsequently transferred to a fraudulent bank account abroad.

Your contacts

Contact us for a review of your business against abest practice benchmark and your industry.

Gianfranco Mautone
Partner,
Forensic Services and
Financial Crime Leader
+41 79 416 76 88
gianfranco.mautone@pwc.ch

Ralf Baumberger
Partner,
Forensic and
Compliance Services
+41 58 792 17 63
ralf.baumberger@pwc.ch

Understanding your organisation's readiness is essential if you want to take proactive steps to protect your business investment and mitigate your risk of fraud.

pwc