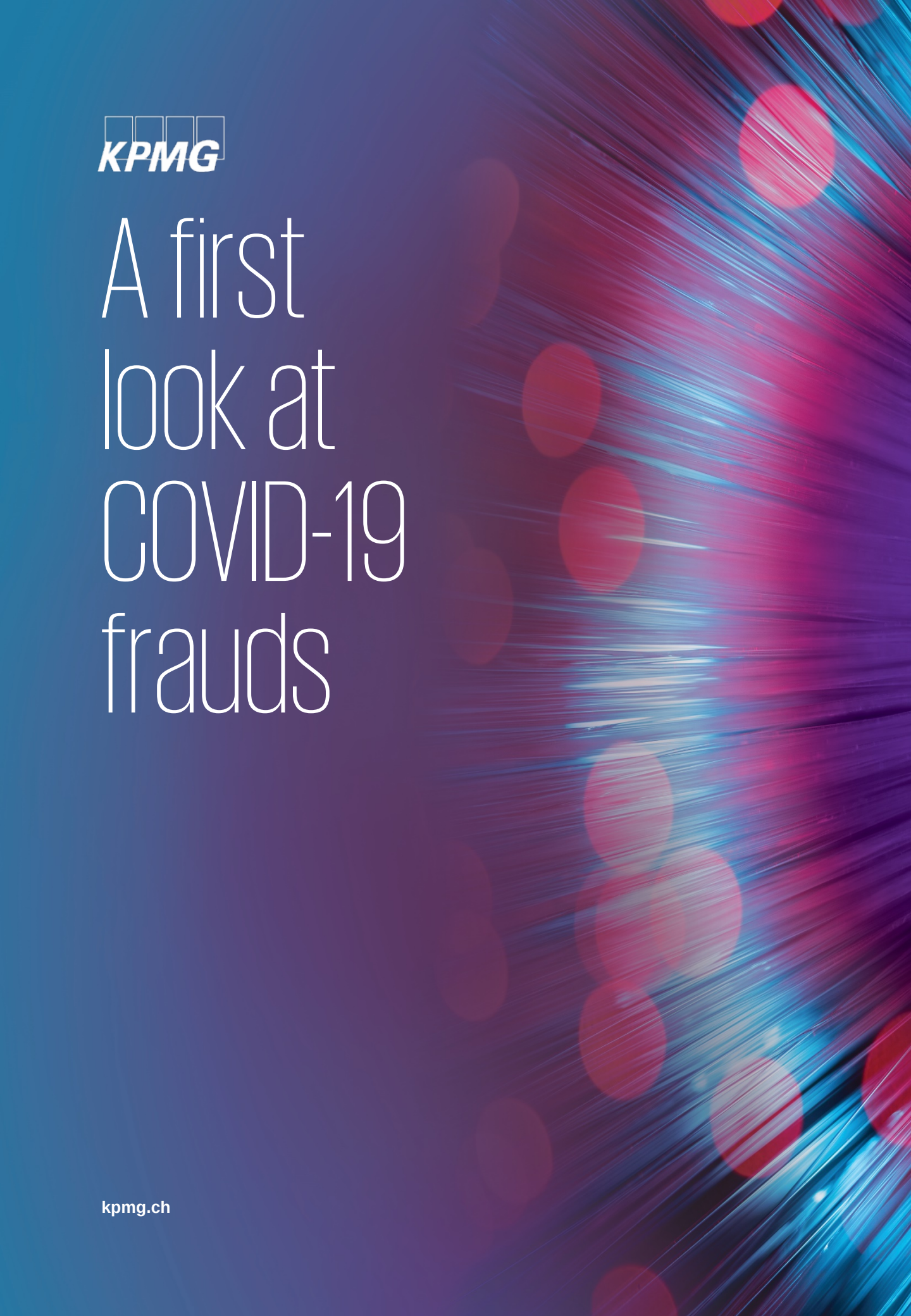
KPMG

A first look at COVID-19 frauds



kpmg.ch

COVID-19 is first and foremost a public health emergency. However, we are seeing a sharp increase in the number of actual and attempted frauds and scams seeking to take advantage of the crisis. In this time of disruption and uncertainty it is more important than ever to ensure that you and your organisation are fully aware of the latest tricks being employed by the fraudsters as well as how to strengthen your controls and how to minimize the risk exposure and damages.

An effective fraud requires both an opportunity for the fraudster and a control weakness on behalf of the victim. The current global situation is helping to create both of these conditions in abundance.

Opportunities for fraud

Disruption and uncertainty often create opportunities for fraud. At short notice, businesses and individuals are working under unusual conditions, with unfamiliar counterparties, facing urgent deadlines and with limited ability to forecast what will happen in the near future. For example, many companies have a new and urgent need for protective equipment such as gloves and disinfectant gel – how can they be sure that the vendor is genuine?

Many of the fraudsters taking advantage of the crisis are experienced at doing so, and are simply adapting their existing techniques to fit the current situation.

At the same time, financial distress gives greater incentives for employees, suppliers, customers, agents and others to commit fraud.

Control challenges

Good controls can prevent fraud but they must be executed consistently by personnel with an appropriate understanding of business risks. Widespread staff absence due to illness or self-isolation means that, in many cases, people are taking on new and unfamiliar responsibilities. Management, meanwhile, are focussed on the immediate needs of keeping the business operational.

Additionally, hastily activated remote working conditions have placed increased strain on the control environments of most organisations which are not always designed to be applied in home office situation. The lack of face-to-face communication means that people rely all the more on electronic communications, and can't so easily ask a colleague for a second opinion.

Together, these factors increase the vulnerability of a business to fraud. One way to counter this threat is to be fully aware of the risks that you face. KPMG routinely monitors active frauds and in this document we summarise the current situation.

COVID-19 fraud examples

France

A French school of engineering's name was used, without their consent, to certify the conformity of masks.

After being informed by a Italian pharmacist and an Hungarian company they discover the fraud and enforced legal actions.….

Netherlands

Dutch police took 10 fake web shops offline after they offered products such as COVID-19 tracker apps and anti-bacterial credit cards. Some had cloned the identities of legitimate shops.

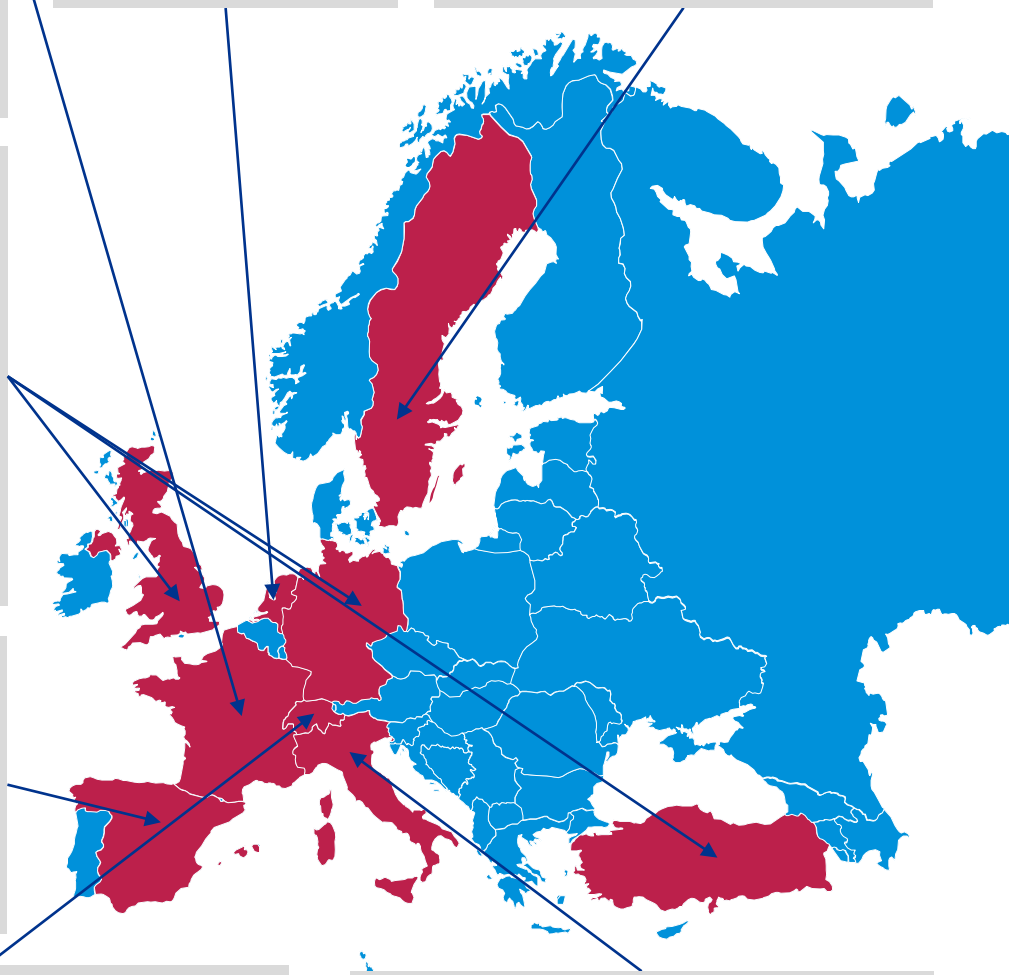
Sweden

SMS messages were sent to solicit donations on behalf of the Karolinska University Hospital for coronavirus research. Only Bitcoin were accepted making it very difficult to trace the scammer.

Imposters have stolen valuables under the pretence of installing 'Corona filters'.

UK / Germany / Turkey

During the mayhem caused by the pandemic, companies around the world placed orders to acquire masks from all available sources; and it turned out that the supply never existed. Fraudsters disappeared after obtaining a prepayment leaving companies with over EUR 20m in losses…



Spain

The Spanish government had to return 9,000 ineffective COVID-19 testing kits after buying them from an unauthorised and unlicensed company in China.

Switzerland

The Reporting and Analysis Centre for Information Assurance has detected large numbers of phishing and ransomware attempts linked to COVID-19. Some are sent in the name of the Federal Office for Public Health.

In addition, in March 2020 fishing attack was orchestrated against World Health Organization in which the fraudsters impersonated WHO to steal Bitcoin Covid-19 donations originally collected for the WHO's COVID-19 Solidarity Response Fund.

Italy

False declarations have been made to obtain government grants intended to support businesses during the pandemic.

Police have warned that people knocking on doors claiming to be testing for Coronavirus are actually seeking to steal valuables from the elderly.

Criminal organisations are thought to be taking advantage of the crisis to infiltrate vulnerable sectors of the economy such as through buying hotels.

COVID-19 fraud in detail

Phishing and cyber-attacks

Many scams start out with an email - while some are easy to spot, others can be quite convincing, with correct logos, appropriate language and even coming from a plausible address. We are aware of fraudsters impersonating entities such as airlines offering a refund, national tax authorities offering a tax rebate, and even the Switzerland's Bundesamt für Gesundheit (see example below).

Clicking on a link in the message can download malware to gather corporate information or encourage the recipient to disclose their password. A further threat is the resurgence of 'ransomware'; software that encrypts your data leaving it unusable unless a large payment is made.

CEO fraud & payment diversion

A variant of the email scam is 'CEO fraud', in which an external party impersonates a senior manager and instructs a member of staff to, for instance, make a payment to the fraudster. The message is often worded to encourage the recipient to bypass normal financial controls.

Another technique is to contact a company, to request an urgent payment or pretending to be from a major supplier and provide new bank account numbers. Stated reasons include the real account '*being frozen by a foreign government*'. The next time a routine payment is made it could go straight to the fraudster.

These approaches are increasingly effective at a time when more and more business is being done by email and while people are under greater-than-usual stress.

Countermeasures include raising employee awareness, configuring email systems to flag external senders and enforcing controls at the system level (so that, for instance, a single individual cannot approve an outgoing payment or change vendor standing data). The Swiss National Cyber Security Centre has produced guidance for securing a home office environment[1].

Counterfeit or ineffective products

Supplying personal protective equipment (PPE), disinfectants and medicines is currently big business. However, some fraudsters are seeking to cash-in by selling substandard or fake products. In more normal times, a business might have a lasting relationship with its key suppliers. One characteristic of the COVID-19 crisis, though, is businesses trying to source essential supplies from wherever they can.

Such a hurry cannot excuse the lack of third party due diligences and the very damaging effects such omission may cost a company. During a crisis organisation should double up their vigilance and act with utmost precautions as many fraudsters are attempting to seize the opportunities created by the sense of urgency.

1. https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff-enduser.html

Brand trademark misappropriation

Fraudsters are becoming increasingly creative by coming up with new techniques and targeting industries and organizations that one would think not to be in danger of a Covid-19 fraud. As similar as identity theft aiming at individuals, fraudsters are also stealing your organization's trademark for malicious purposes.

In recent weeks, European bodies have reported that several certificates of conformity issued for protective masks were, in fact, forgeries. Some of those certificates were "issued" by completely bogus certification entities or were using existing brands without the owners' consents.

A recent case was reported by a French School of engineering whose name and address were used on the certificates[2]. The forged certification appears to be fabricated and operated by a British intermediary selling Chinese masks on the European market. The fraud was discovered when the director of the School was contacted by potential buyers requesting the engineering school to confirm the accreditation.

This case illustrates clearly how an institution, regardless of its size and nature, is vulnerable and may become a victim of opportunistic fraudsters. Besides, it shows that a good practice is to conduct at least basic due diligence even in period of crisis.

CERTIFICATE

With EU Directive of Personal Protective Equipment 2016/425

Certificate No.: CE-20-0324-05

Holder: Jiaxing Kanghuang Electronic Technology Co., Ltd

East floor 2, building 1, Yongxing North Road, industrial zone, zhouquan Town, Tongxiang City, Jiaxing City, Zhejiang Province

Product: Self priming filter type anti particle respirator (kn95)

CE

Certification Body

For and on behalf of EUROSCENE BUSINESS SOLUTIONS CO.,LTD

Authorized Signature(s)

Euroscene Business Solutions

Date: Mar.24.2020

The CE marking may be used if all relevant and effective EC directives are complied with.

Euroscene Business Solutions Limited

Ecole Supérieure du Bois rue Christian Pauc BP 10605

44306 Nantes cédex France

2. https://www.francetvinfo.fr/sante/maladie/coronavirus/masques-respiratoires-un-organisme-nantais-porte-plainte-apres-la-decouverte-d-un-faux-certificat-de-conformite-emis-a-son-nom_3932955.html

Supply scams

We've also seen fake websites that seek to take advantage of these same supply shortages for essential goods. Rather than providing fake products, these websites simply pocket the money before disappearing. The police in the Netherlands recently disabled 10 such online shops, some of which used the names of legitimate retailers. Meanwhile, a UK company lost over £15,000 over a bulk consignment of protective face masks that were never delivered.

Victimized public and non-profit sectors

Many organisations want to support their community at times such as this through a charitable donation. However, we have seen that fraudsters are taking advantage of this philanthropy by creating fake charities.

In one example, donations were solicited on behalf of a well-known hospital in Sweden to support coronavirus research. Only Bitcoin were accepted, making it very difficult to trace the fraudulent recipient.

Non-profit organizations are also exposed to financial and reputational risks. Example is March 2020 fishing attack in which the fraudsters impersonated World Health Organization to steal Bitcoin COVID-19 donations originally collected for the WHO's COVID-19 Solidarity Response Fund.

Bribery risks

There is often an increased risk of bribery when people are placed in difficult situations. This is likely to be of most concern for businesses with overseas operations, but domestic issues should not be entirely discounted.

For example, a manufacturing business operating in an industry where supply chains have come under pressure due to COVID-19 restrictions should be alert to employees accepting money or other benefits to prioritise supplying a particular customer.

Likewise, staff working in an overseas subsidiary may face pressure to make facilitation payments or bribes to release imported items from customs checkpoints or to continue to operate during a lockdown. The Anti-Corruption Resource Centre found that during the 2014 Ebola crisis, residents in Liberia were commonly bribing soldiers and police officers to evade quarantine[3].

Of particular note, some business that normally consider themselves to have a low corruption risk may come into increasing contact with foreign government officials. Bribing government officials is specifically targeted by the US FCPA.

---

3. https://www.cmi.no/publications/file/5522-ebola-and-corruption.pdf

Typology of frauds

Most prevalent cases of fraud during the Covid-19 crisis

Phishing and cyberattacks

Clicking on a link in an email that allows fraudster to access your network and that might lead to a massive data leakage or the blockage of your operations.

CEO Frauds & Charity scams

Fraudsters impersonating senior managements and instructing junior staff members to proceed urgent payments on their behalf or setting up bogus charity calling for the generosity of the general public.

Counterfeits & supply scams

The sudden rise in demand for masks gave fraudsters an opportunity to market fake products or to simply advertise sought-after products and vanish with the money.

Trademark misappropriation

Racing to market highly demanded goods, manufacturers are tempted to use and promote forged certifications and certifications without the consent of the owner of the intellectual property.

Bribery and corruption

Real suppliers asking for extra payment in order to send demanded goods or purchasers offering incentives to secure a delivery is on the rise.

Financial market abuses

Taking opportunity of the current mayhem, investors may be lured into manipulating the price of lower-volatility securities or using non-public material information when trading.

KPMG and you

Investigations services:

- Fact-finding investigations on all types of white collar-crime and misconduct: fraud, corruption or violation of laws and regulations
- Identification of the perpetrators, quantification of the damages, allocation of responsibilities and assistance with recovering assets
- Crisis management by taking immediate or emergency actions

Corporate Intelligence services:

- Essential for effective third-party risk management and mitigation of commercial, reputational and regulatory risks
- Quick and discrete background profile on your current or future counterparty – business partner, customer, debtor or future employee
- Clear and consistent reporting of key risk issues and indication of risk factors

Dispute Advisory services:

- Assessment and quantification of operational losses and damages, also suffered due to COVID-19 crisis
- Expertise in handling any kind of financial and accounting aspects of disputes

Forensic Technology services::

- Incident Response Services in the event of a cyber attack
- Assistance with locating, securing and analyzing relevant or affected data
- e-Discovery to help you locate relevant documents and information
- Assistance in the evaluation of datasets using forensic data analysis

Corporate Compliance services:

- Development, assessment, reinforcement and support of your compliance program to fully uphold your corporate values and ethical standards
- Code of Conduct and policy development
- Risk assessment and monitoring
- Implementation and operational support
- Ethics and Compliance training and change management

Anti-Bribery & Corruption services:

- Support in preventing, uncovering and handling cases of bribery and corruption
- Development of solid and tailored anti-bribery and corruption compliance programs (e.g. following ISO 37001)
- Review of the internal controls framework and anti-bribery and corruption risk assessment

Contacts

Anne van Heerden
Partner, Head of Forensic
KPMG Zürich

+41 58 249 28 61
annevanheerden@kpmg.com

Philippe Fleury
Partner, Financial Services
KPMG Geneva

+41 58 249 37 53
pfleury@kpmg.com

Eric Blot
Director, Forensic
KPMG Geneva

+41 58 249 37 24
eblot@kpmg.com

Erwin Frank Barentsen
Director, Forensic
KPMG Zürich

+41 79 708 17 16
ebarentsen@kpmg.com

kpmg.ch