FRAUD Patterns

Status as of: 12.08.2020

Developed primarily based on public sources, supplemented with observations from client conversations and past crisis experience

Claudia Nestler
Partner, Forensic Services
Frankfurt am Main
+49 175 2980952
claudia.nestler@pwc.com

Jane He
Senior Manager, Forensic Services
Frankfurt am Main
+49 151 22898663
qian.x.he@pwc.com

Christoph Hornbach
Senior Associate, Forensic Services
Frankfurt am Main
+49 151 16739234
christoph.hornbach@pwc.com

About this document

This document contains current fraud trends and analysis in the context of COVID-19. The source of the analysis includes publicly available information (i.e. media articles), client conversations and our forensic experience. PwC Germany Forensics Team updates this overview on a regular basis.

Fraud patterns overview

Industry \ Type of fraud	1| Business partner fraud	2| Tapping of govern-ment funds	3| CEO-/ supplier fraud	4| Bribery and corruption	5| Money laundering	6| Accoun-ting fraud	7| Antitrust violations	8| Mgmt Override	9| Cyber
Auto-motive	low	medium	medium			low	low	low	medium
Financial Services	low		medium		low	low	low	low	medium
Ind. Manu-facturing	low		medium		low	low	low	low	medium
Insurance	low		medium			low	low	low	medium
Pharma & Healthcare	low		low	low	low	low	low	low	high
Public Services		high		low				low	medium
Retail & Consumer	low		medium		low	low	low	low	medium
Transport & Logistics	low		medium		low	low	low	low	medium

high reporting medium reporting low reporting

1 | Business partner fraud

Fake-Shops

Industry: Pharma & Healthcare

The number of cases of consumer fraud increased significantly during the COVID-19 pandemic. One driver is the current shortage of many urgently needed commodities, especially in the medical sector (protective equipment and disinfectants), which lead to the opening of many dubious online shops. For better deception often names of real existing companies are used (e.g. pharmacies, medical device companies). The fake shops advertise with a high stock of currently scarce goods.

Besides, fraudsters are also approaching companies directly in a targeted manner and offering protective clothing. Here as well, fraudsters often act under the names of real existing companies, only changing the account number for invoices. Clients are asked to pay - at least partially - upfront. The ordered items are never delivered.

Counterfeiting of products

Industry: Pharma & Healthcare

Another driver for the rise in consumer fraud is the increased demand for medical goods due to the current shortage of supply. Fraudsters are currently selling a large number of counterfeit products from this area. These include ineffective counterfeit medicines or masks that do not filter viruses. Meanwhile, China has confiscated 31 million fake masks. The large sales platforms are also increasingly being used to sell counterfeit products. Amazon has removed over a million products from the platform that have made false claims about the virus. To prove the authenticity of their counterfeit products, fraudsters are increasingly forging certificates from real testing facilities.

Missing/lack of verification of business partners

Industry: All

Due to the current shortage of many goods and inputs, companies are often forced to enter into new supply relationships. Given the current situation, there is not enough time and resources available for a precise and proper review of the business partners before onboarding and monitoring. Especially with the accumulation of dubious suppliers, this represents a risk for companies.

Insurance fraud

Industry: Insurance

The number of received damage reports at insurance companies is expected to increase in the current situation. In addition, insurers are also required to process their customers' requests quickly. During times of economic hardship, individuals and companies might file false claims:

- Submitting fraudulent medical claims;
- Submitting inaccurate or exaggerated expected financial gains with respect to a business interruption coverage;
- Submitting claims based on alleged damage to the company's vehicle fleet;
- Targeted arson in company buildings to file a claim;
- Submitting claims for phantom assets following a fake burglary.

2 | Tapping of government funds

Fraud in relation to short-time work (Kurzarbeitergeld)

Industry: Public Sector

The following schemes have been identified:

- Fraudsters apply for short-time work compensation for employees and allow them to continue working to the same extent as before. This is facilitated by home office arrangements where the recording of hours is more difficult;
- Employment of family and friends at short notice to receive additional short-time work compensation;
- More companies than ever before are applying for short-time work (1m+ since March). The volume makes it difficult to prevent and detect fraud.

Fraud in relation to COVID-19 emergency aid/support

Industry: Public Sector

The support measures introduced by the federal state and the single states has led to many cases of fraudulent applications. At the same time, application reviewers have instructed to process the applications in a timely manner. Several other factors also make it easier for fraudsters:

- Often no verification of the tax numbers for authenticity;
- Submitted information on liquidity does not need to be verified by supporting documents (only reasonableness checks);
- Process weaknesses within the government sector already led to double payments or payments to non-existent companies.

The following potential schemes have been identified:

- Fraudsters obtain company information from publicly available sources and apply in the name of an existing company. In the application, they use their own bank account to receive the money;
- As some processes do not involve checks on unique identifiers like tax IDs, fraudsters apply for support with fake company details;
- Fraudsters just founded a company to receive the governmental support;
- A real existing company might apply for support measures. However, the director applying on behalf of the company uses his private bank account to receive the money;
- An already insolvent company applies for support. If the insolvency is neither disclosed nor discovered by the reviewer, the money might be transferred and becomes part of overall assets that need to be distributed among all creditors;
- A company that was already in trouble before the COVID-19 crisis applies for support and later files for insolvency. As for an already insolvent company, the money that was paid out might be lost;
- Use of dormant company to apply for support;
- Fraudsters pose as the funding institution in e-mails and demand repayment of the emergency aid;
- Fraudsters use third parties often living in difficult financial circumstances as financial agents. These apply for emergency aid without actual legitimacy and provide their account details. After the money is received, the money is passed on immediately, usually in cash.

First findings suggest that states that run their processes completely digital are more heavily targeted by fraudsters. Banks have already reported incoming government money on newly opened or private bank accounts to the authorities.

Fraud in relation to government loans

Industry: Public Sector | Financial Services

In contrast to governmental support that is directly handled by the states or state-owned banks, financial support via government loans requires an existing Hausbank relationship. This mitigates some of the schemes outlined above. However, private banks were urged to be not too strict when examining loan applications. This provides opportunities for fraudsters to:

- Capitalization of dormant shelf companies;
- Manipulation of business figures.

Besides, adherence to the terms and conditions under which the loans were granted (i.e. salary caps and prohibition of dividend payments) needs to be monitored on an ongoing basis.

Fraud in relation to BAFA Grant for Consultancy

Freelancers and SMEs which have got into financial difficulties due to Corona can apply at the BAFA for a grant of 4,000 € for consultancy services. The grant is transferred directly from BAFA to the consultants, who must first be accredited by BAFA. During the recent weeks, more than 9000 applications for accreditation have been received. This support has now prompted many so-called consultants with doubtful qualifications to offer their services to companies and freelancers en masse, as their services are paid in full by BAFA up to a value of 4000 €.

3 | CEO/CFO- and supplier fraud

Accumulation of CEO/CFO-Fraud

Industry: All

CEO-Fraud is a type of fraud, where criminals pretend to be high level executives and give employees urgent orders via E-Mail or WhatsApp to transfer money. In addition, fraudsters use language software to pose as high-level executives on the telephone. The COVID-19 pandemic forces companies to adjust processes and coordinate interactions. Fraudsters use the resulting uncertainties. There has already been an increase in the number of CEO-Frauds. Companies are currently especially vulnerable as instructions have in many cases to be given via email or phone as people work remotely.

Supplier fraud is related to CEO/CFO-Frauds. Fraudsters send fake bills in the name of real suppliers of the company. This type is expected to be more frequently used than CEO/CFO-Frauds during Covid-19 pandemic.

4 | Bribery and corruption

Employee bribery

Industry: Healthcare I Public Sector

The scarcity of medical goods and the simultaneous increase in demand for these goods can lead to attempts to bribe employees of the manufacturers of these goods. This can be further exacerbated by the ramp-up of many production facilities, as companies must provide sufficient protective equipment to open their sites.

Due to the intensive research on a corona vaccine, there is currently also an increased risk that research employees will be bribed to pass on research documents. This risk is currently very high, as it can be assumed that the company which is the first to bring an effective vaccine to the market can expect very high profits.

Furthermore, the current delays in supply chains may increase the risk of corruption in some countries. Urgently needed goods might be detained by the authorities and only released against a bribe.

Besides, through the Corona aid packages worth billions, the OSCE now also warns of an increase in corruption. In many countries, the authorities could be overwhelmed with the distribution and criminals could take advantage of this. There is also an increased risk of corruption among officials who coordinate the distribution of aid funds or are responsible for purchasing medical equipment. First cases of corruption in connection with the purchase of medical equipment were already reported in Honduras, Brazil and Malaysia.

5 | Money laundering

Accumulation of money laundering activities

Industry: All

The current crisis creates some incentives for criminals to increase their money laundering activities:

- Changing processes in the crisis
  - Banks temporarily switched to remote working and some have restricted in-person services leading to potential process deficiencies to verify customers' identities properly;
  - Some client population segments (i.e. seniors) are not familiar with the use of online-platforms and which can be exploited by fraudsters (e.g. using their data to open new accounts for AML);
  - Relaxation by the BMF of the examination obligations for the prevention of money laundering in the case of supportive loans.
- Government support funds exploitation
  - Funds from illegal applications for government funds must be introduced into the system;
  - Government officials in countries with low control processes, transparency and accountability measures might divert government support funds in their own bank accounts.

- Using the crisis situation
  - Use of illegally acquired funds to purchase or produce medical goods;
  - Increase of fraudulent activities is recognized during the crisis, these funds must be introduced to the system;
  - Acquisition of insolvent restaurants or bars for subsequent money laundering purpose;
  - Acquisition of cheap real estate for subsequent money laundering purpose;
  - Exploiting the increased use of banknotes
    - large amounts of re-deposits are expected to be made after the crisis, this enables criminals to infiltrate their money,
    - acquisition of real assets (e.g. gold), which are less easily traceable,
    - general growth of cash funds transactions lead hinders traceability and controllability.

6 | Accounting fraud

Accumulation of falsified balance sheets

Industry: All

The federal and state subsidy programs set up because of the coronavirus pandemic create incentives for companies to manipulate their financial statements in order to qualify for support. Besides, companies are confronted with losses and might not meet financial targets or market expectations. Financial statement fraud might become an important aspect for the upcoming audits.

Examples of typical patterns to look for include premature recognition of revenue, deferral of expenses, premature recognition of WIP for capital projects, inaccurate booking in suspense accounts, inaccurate estimation for depreciation, impairment and provisions, unusual changes to accounting policies for estimation, unusual change or booking to intercompany receivables and payables, etc.

7 | Antitrust violations (competition and antitrust laws)

Limited cooperation among businesses

Industry: All, focus on pharma

To avoid a supply shortage during the COVID-19 pandemic, companies are now allowed to cooperate with each other for distribution of scarce goods. Under those conditions, companies are allowed to coordinate actions such as production, warehousing and distribution which would under usual conditions be regarded as a violation of antitrust laws.

The EU Commission has issued a Temporary Framework which sets out the main criteria that the Commission will follow in assessing these potential collaborations. Companies are responsible for assessing the legality of their cooperation themselves. The Commission has been and will be supporting companies and trade associations to assess the legacy of their collaboration plans. In exceptional cases the Commission will provide companies with Comfort Letters regarding concrete collaboration plans. With the Comfort Letter, the EU Commission gives its official approval for the collaboration project. The first Comfort Letter has been provided to “Medicines of Europe”. The current possibility of limited cooperation could also be abused by companies to increase their profits. In particular, the effects of the COVID-19 pandemic, which has put many companies in financial difficulties, could encourage companies to enter into illegal agreements.

8 | Management override (internal control weaknesses)

Changes of the internal control

Industry: All

The increased work in the home office can lead to changes in process flows in companies. On the one hand, it can lead to a change in roles and responsibilities within the framework of process flows and internal controls with changes in authorizations. On the other hand, there may also be a change in monitoring or application controls (e.g. change of control frequency). Changes in process and control procedures are often accompanied by an increased risk of fraud, especially in crisis times, when decisions are made under great pressure. At the moment managers have to react quickly to the effects of the crisis, which can increase the risk of "Management Override".

9 | Cybersecurity

Phishing E-Mails

Industry: All

- E-mails regarding information on application for state aid in an attachment which contains trojans and malware;
- E-mails regarding lucrative offers for medical products where the product catalogue contains malware;
- E-mails regarding allegedly new relevant information on COVID-19 with an attachment that contains trojans and malware.

Home Office Fraud

Industry: All

Fraudsters pretend to be IT service staff of the company and inform employees in home office about an alleged security risk in the system. Then they ask their victims to install a specific software to fix the issue. This software grants the fraudsters remote access to the computers and can thus access data and passwords.

Cloud Account Hijacking

Industry: All

Cloud solutions are currently being used by many companies to enable their employees to continue working in home office. Employee accounts are hacked and fraudsters gain access to sensitive company data stored in the cloud.

Fake-Shops

Industry: All

- Fraudsters build exact fake versions of official websites. Malicious software will be installed on customers' computers visiting these websites;
- Fraudsters build exact fake versions of the official application pages for state support and capture data from the application forms with which they in turn submit fake applications to receive governmental support.

Credit Card-Skimming

Industry: All

The coronavirus pandemic has led to a rapid increase in online orders. This has also brought fraudsters to the scene, who are increasingly trying to get information from EC and credit cards. In March, credit card fraud on the web increased by 26%.

Attacks on systems

Industry: Healthcare

Criminals smuggle blackmail software into the infrastructure of medical facilities. These paralyze the entire system of the facilities. Criminals then demand a ransom for the release of the paralyzed system.

Cyber Espionage

Industry: Healthcare

Hackers try to infiltrate the systems of laboratories which work on a vaccine for Covid-19.

10 I Miscellaneous

Securities "Pump and dump"

Industry: All

Fraudsters are buying large amounts of stock in microcaps. Then they spread positive news about the company to pump the stock price up. When the price reaches a certain level the fraudsters sell the stocks again.

Fake COVID-19 medication

Industry: Pharma & Healthcare

Custom agents are confiscating more and more bogus medication that claim to treat COVID-19 disease. In addition, fraudsters have successfully distributed an alleged vaccination against COVID-19 for several weeks via a website that was a replica from the WHO website. Also the name and logo of the Israeli company MIGAL is currently misused by fraudsters for the illegal distribution of COVID-19 vaccination kits. Especially in South America, fake COVID-19 vaccination sets with the MIGAL logo are being sold en masse.

Fake Tracing Apps

Industry: All

Fraudsters develop smartphone apps that claim to track the spread of the virus. However, these apps infect the user's phone with malware and steal personal information once installed.

Fake Charities

Industry: All

Fraudsters call for donations to non-existent charities and, once donated, keep the money to themselves.