Allianz Trade

White-collar crime
new technologies, new horizons of fraud

Current trends, a criminological look
at perpetrator profiles and motives – and the question:
How can companies protect themselves?

Euler Hermes Deutschland
Niederlassung der Euler Hermes SA
22746 Hamburg
Phone +49 (0) 40 / 88 34 - 0
Fax +49 (0) 40 / 88 34 - 77 44
info.de@allianz-trade.com
www.allianz-trade.de

Allianz Trade is the trademark used to designate a range of services provided by Euler Hermes.

The weakest link – the "human factor" as a corporate risk

It remains an inconvenient truth for companies and an underestimated danger: internal perpetrators, i.e., the company's own employees, continue to cause the most and, in total, the highest losses. But external perpetrators are gradually catching up – not least because of the digital transformation and technological developments.

It gets particularly interesting with so-called "social engineering" fraud cases, for example fake president, payment or order fraud. Here, the attempted fraud comes from external perpetrators – but they exploit the weakest link – the "human vulnerability" of employees and manipulate them. And although these scams are not new, although many companies are sensitizing their employees, the number of cases continues to rise.

But why can people be hacked and manipulated? How do the "social engineers" get their victims to carry out demonstrably illegal activities such as bank transfers without the applicable dual control principle? Why do long-serving employees, of all people, often become perpetrators? What motivates them? What are the perpetrator profiles – and above all: How can companies protect themselves?

In an analysis from October 2022, we have already determined: the greatest damage is caused by male perpetrators between the ages of 40 and their mid-50s, educated, in senior or executive positions in the financial sector with at least 10 years of service.

In this guidebook, we have joined forces with legal scholar and criminologist Hendrik Schneider, Prof. PHD in an attempt to explain the motives of white-collar criminals in criminological terms and – based on this – to provide companies with tips on how they can combat white-collar crime and protect themselves (in the best possible way) against attacks by internal and external perpetrators.

Your Allianz Trade-Team

CONTENTS

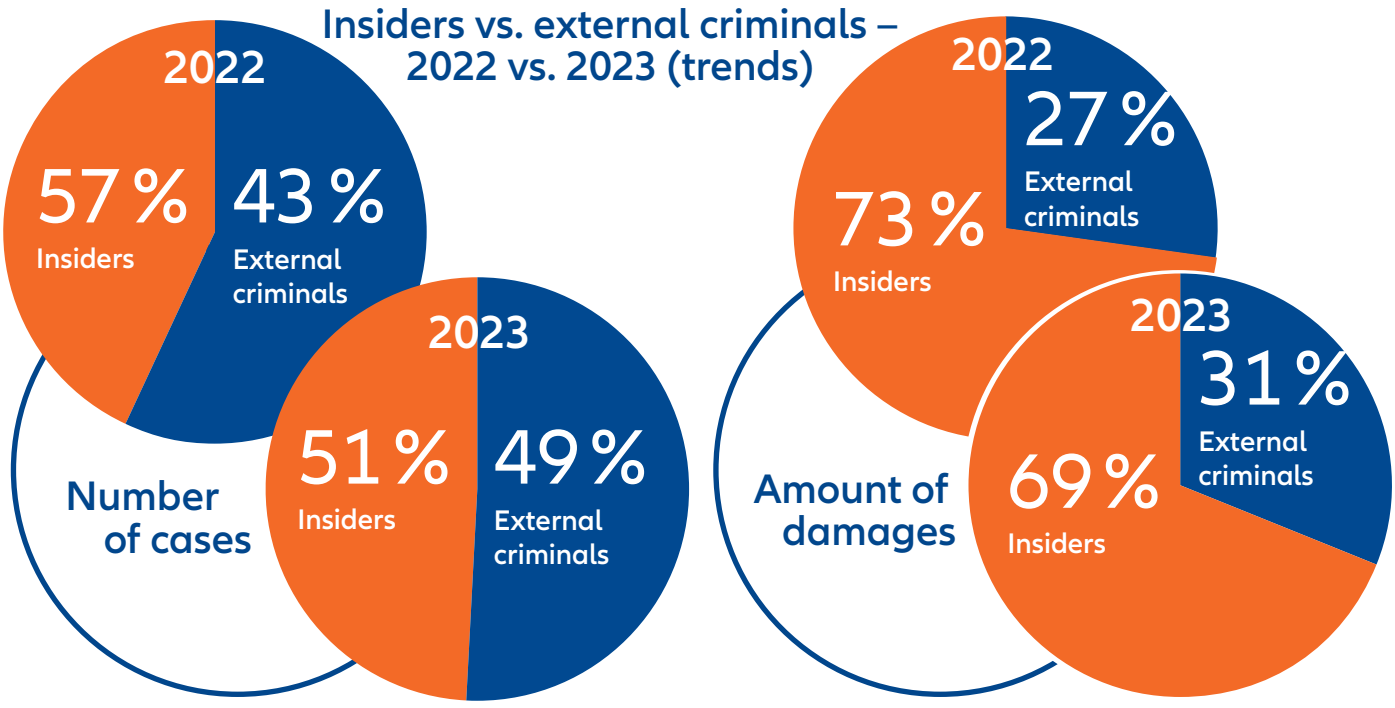
Extract from Allianz Trade
Loss statistics

Allianz Trade's fidelity insurance protects companies against financial losses caused by targeted criminal acts – both by so-called "internal perpetrators" (e.g. employees, temporary workers) and by external third parties (e.g. hackers). A look at our damage statistics provides fascinating insights.

White-collar criminals are surfing the home office wave

White-collar criminals are striking with increasing frequency and significantly more companies are affected than in previous years. In particular, offences by external perpetrators have been rising rapidly recently. In 2022, internal perpetrators caused around 57 % of cases.

In 2023, the picture is different: The share of internal perpetrators has so far been almost balanced at 51 % to 49 % by external perpetrators. In terms of the amount of losses, however, the truth remains uncomfortable for companies: own employees cause the greatest losses. However, external perpetrators are gradually catching up.



Source: Allianz Trade loss statistics

Allianz Trade is the trademark used to designate a range of services provided by Euler Hermes.

Allianz loss statistics show that companies of all sizes and from almost all sectors are affected by social engineering. However, a trend has recently been observed in those sectors which were particularly frequently victims of hackers.

"People Hackers" have been experiencing a boom for years

"Social engineering", i.e. fraud schemes in which perpetrators manipulate people, have been experiencing a boom for many years. This scam now accounts for around one quarter of all claims reported to Allianz Trade.

Social engineering fraud cases increased by about 18 % in 2022 compared to the previous year. This trend continues in 2023 year to date.

+ 400 %
Social engineering fraud cases have increased fivefold since 2014

+ 18 %
Increase in social engineering fraud cases 2022 vs. 2021

In particular, payment fraud (payment diversion), i.e. the diversion of money flows, has become increasingly popular in the portfolio of white-collar criminals, who are also taking advantage of constant technological progress.

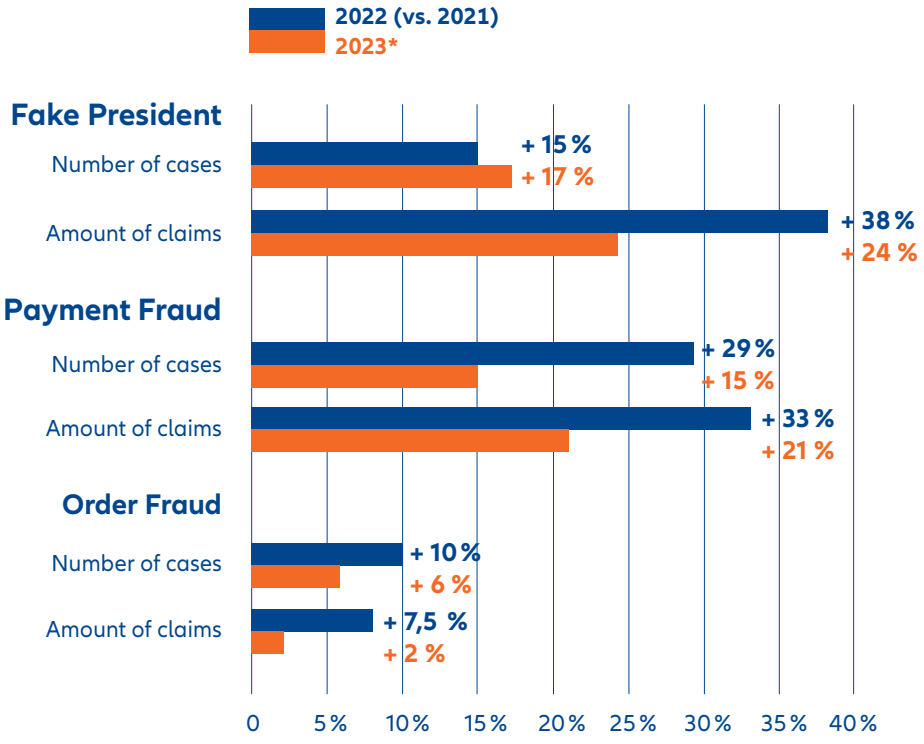
Source: Allianz Trade loss statistics

Fake Presidents come into vogue again

What is particularly interesting is that since 2022, the "fake president" scam has been experiencing a revival. In 2022, losses caused by fake presidents recorded a 38 % increase, while the number of cases increased by 15 %.

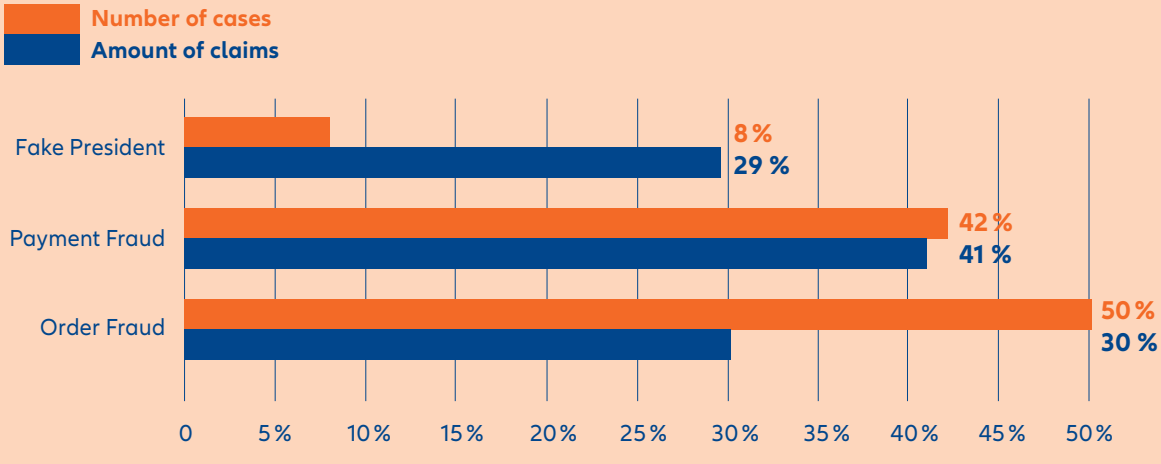
For many years before that, the number of cases stagnated and the amount of losses per case gradually declined. In most cases of "fake president" fraud, the loss amounts are now only in the high six-digit or low single-digit million range. Between 2014 and 2017, the fraudsters often still caused losses of between EUR 10 million and EUR 50 million.

Trends in figures: Changes in number of cases and amount of claims



**Allianz Trade Estimate based on H1 2023*

Payment fraud causes the greatest losses overall in 2022



Source: Allianz Trade statistics

Allianz Trade is the trademark used to designate a range of services provided by Euler Hermes.

73,144

White-collar crimes recorded by the BKA in Germany in 2022 (+ 42.6 %).

Source: Police crime statistics 2023

15 %

The companies affected reported losses of more than EUR 1 million, which means an increase of 50 % compared to 2020.

Source: KMPG, Study White-collar crime in Germany 2023

2.1 billion euros

was lost by businesses in Germany due to white-collar crime in 2022.

Source: Statista, July 2023

81 %

of German companies rate the risk of white-collar crime **for other companies** as high.

Source: KMPG, Study White-collar crime in Germany 2023

34 %

of the companies rate the risk of being affected by of white-collar crime **themselves** as high.

Quelle: KMPG, Study White-collar crime in Germany 2023

White collar crime: further increase in the number of cases

The losses caused by white-collar crime are high. Many companies see the danger, but more for others than for themselves. Phishing scams continue to rise strongly. In addition to ransomware, however, there are also social engineering scams still on the rise, mainly due to artificial intelligence such as ChatGPT.

26 %

of successful cyberattacks on German companies were "social engineering" cases such as Fake President. Together with phishing and ransomware, social engineering forms the top 3 fraud schemes.

Source: TÜV Cybersecurity Study 2023

2.7 Mrd. USD

in losses were incurred by around 22,000 companies worldwide due to social engineering in 2022, an increase of 14 % compared to the previous year.

Source: FBI Internet Crime Report 2023

38 %

The amount of losses caused by Fake President suddenly recorded a 38 % increase in 2022 again.

Source: Allianz Trade loss statistics

57 %

Internal perpetrators are involved in 57 % of all white-collar crimes, and in 31 % of the cases they commit the crime on their own.

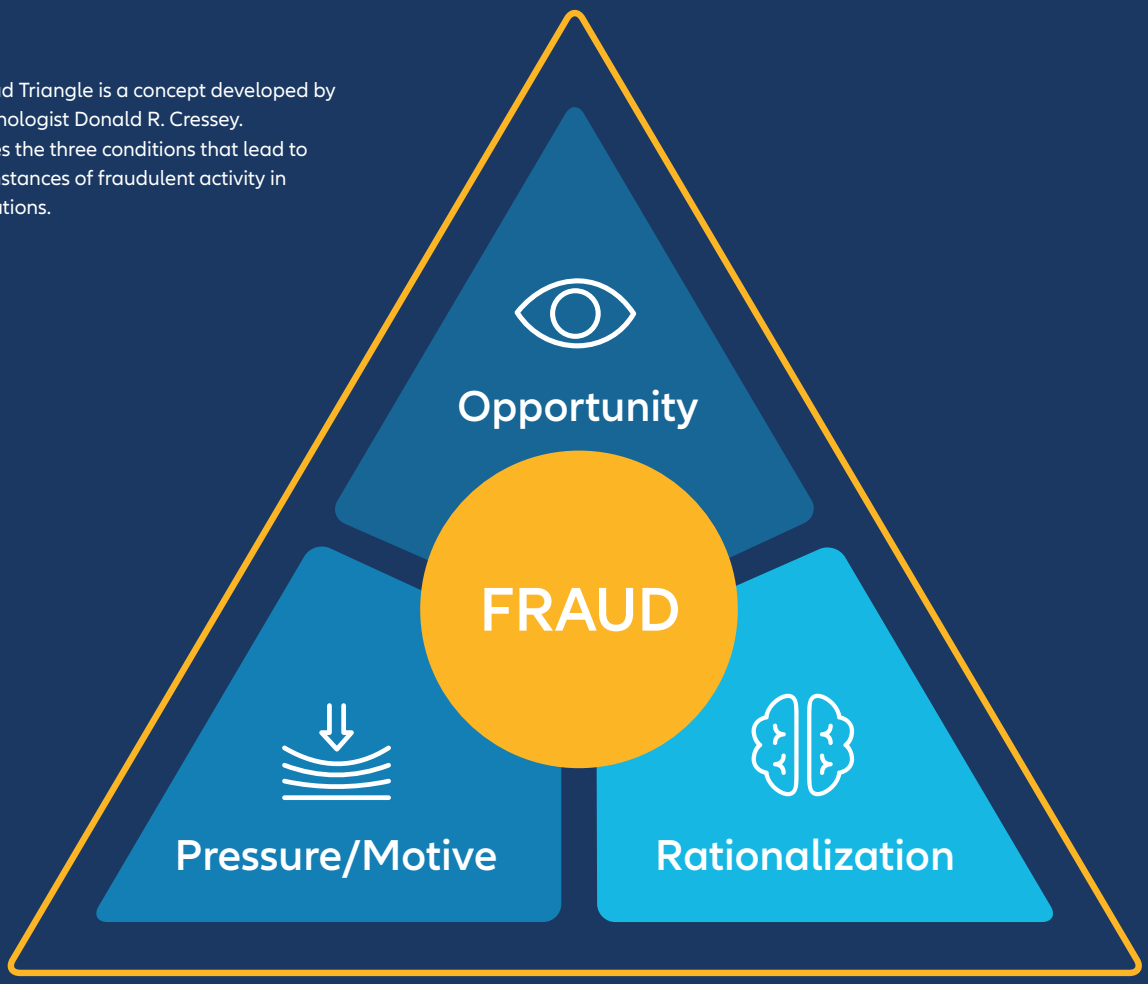
Source: PWC, Study White-collar crime 2022

46 %

of companies worldwide were victims of white-collar crime in the years 2021 to 2022; in Germany, the figure was around 40 %.

Source: PWC, Study White-collar crime 2022

The Fraud Triangle is a concept developed by US criminologist Donald R. Cressey. It outlines the three conditions that lead to higher instances of fraudulent activity in organizations.



Why do employees become perpetrators?

A well-known proverb says: "Opportunity makes the thief". But that can only be half the truth, because, not everyone automatically commits a criminal act just because there is an opportunity to do so. So what else contributes to people becoming offenders? And to what extent can companies counteract this?

Allianz Trade is the trademark used to designate a range of services provided by Euler Hermes.

The well-known "Fraud Triangle"[1] of criminologist Donald R. Cressey provides some interesting starting points. According to him, three factors must be present at the same time: an opportunity to commit a crime, pressure (or a corresponding motivation) and "rationalization", i.e. the justification of one's own crime. Opportunity is certainly the best known aspect – it is obvious that without opportunity a crime cannot take place. At the same time, however, a perpetrator must also have the necessary competence and be able to assume that there is only a small probability of being discovered. In the prevention of white-collar crime, this aspect has often played a key role up to now: companies are strengthening their internal control mechanisms in order to reduce the incidence of crime.

For people to become criminals, however, it usually takes more than that. In most cases, it is considerable pressure. This can have many facets: time pressure, pressure to perform, pressure to find solutions, lack of resources, hierarchical, social or emotional pressure, peer pressure, pressure to please, pressure of expectations (from others or from oneself) and, of course, financial pressure can all be responsible for a person becoming an offender.

Cressey also describes pressure as "non-sharable information"[2]. This means that a person perceives a life situation as so shameful that he or she does not dare to deal with it openly or share it with those around him or her. This can be financial hardship, addiction to gambling or shopping, or the shame that intimacies are made public, as in the "pig butchering" scam.

Many fraud schemes, especially "social engineering", start precisely here. In the well-known "fake president" scam, for example, criminals pose as superiors and trick employees into making large money transfers: The scam works because it touches people at their core. It starts precisely where people connect – for example, in the form of appreciation, which everyone intrinsically seeks. But other facets of pressure, such as the pretence of a supposed crisis situation, can also play a decisive role.

The third side of the "devil's triangle" is justification. When people do something that is not okay, they have to justify it internally in order to maintain their own self-image. "I work so much, I deserve this" or: "I am the real victim, and this is actually due to me" or: "This is not hurting the company now" or: "This was demanded of me".

The inner coping and justification strategies are manifold, but often difficult to see through from the outside. Only in rare cases, such as in court proceedings, do they come to light at all – and even then only in rudimentary form. Moreover, there are certain perpetrator profiles[3] and personality structures[4] in which this justification is only very slightly pronounced.

Nevertheless, it is worthwhile for companies to take these two aspects, which have often been neglected up to now, into account in their prevention efforts. This is because the corporate and error culture in particular play a major role here: very authoritarian management styles, an absolute focus on results ("whatever the cost") or a "just do it, no matter how" culture can significantly promote white-collar crime. A healthy error culture and a good balance between control and trust (see also pages 20/21), on the other hand, can significantly reduce the risk of criminal employees.

[1] Cressey, D. R. (1953), Other people's money; a study of the social psychology of embezzlement

[2] Cressey, D. R., The Criminal Violation of Financial Trust, American Sociological Review Volume: 15 (1950), pp. 738–743

[3] Prof. Dr. Henridk Schneider/Rölfs WP Partner AG (2009), Der Wirtschaftsstraftäter in seinen sozialen Bezügen

[4] Benjamin Schorn (2022), Gier, Macht, Scham – Motive krimineller Manager psychologisch erklärt

New technologies – New (fraud) horizons

New technologies, artificial intelligence and applications like Chat GPT are a quantum leap in the use of data and have many advantages. Many processes can be simplified or made more efficient. But there is a flip side to the coin: they also make it easier for fraudsters. Particularly when it comes to "social engineering," the manipulation of people, this harbours many risks.

Fraudsters do not sleep, they move with the times and use all the technologies at their disposal. For example, Allianz Trade had its first fake presidential case a few years ago, in which we assume that audio deepfakes were used. Since then, there have been isolated cases where voice forgery could not be ruled out, but where the evidence was much less clear. The time and the technology - at least on a broad scale – were probably not yet ready for a large scale, and the effort was probably still too high.

Audio Deepfakes: Software with a quantum leap in the last years

But: the freely available software for cloning voices has made a quantum leap in recent years. Gone are the times in which the voice from the tape sounded tinny and, even with poor cell-phone connections, there was not too much risk of confusion in most cases. However, a current self-experiment (try it out!) with relevant AI programs ends with fascinating and at the same time frightening results. So it should only be a matter of time before these applications find their way into widespread use. The "break even" point at which an application is worthwhile for fraudsters should not be far off.

Fake President Cases: Rising numbers again – and the associated question of "why"

can also be done in the classic way, without any audio: in the fake president scam, e.g. a fraudster poses as a supposed supervisor who induces employees to make big money transfers. Last year, Allianz Trade again recorded an increase in these classic fake president cases, bucking the trend of previous years (stagnating case numbers for this scam and lower loss amounts than at the time of the "peak incidence" with record losses of over 50 million euros). So now there is an increase again – and the associated question of why.

Chat GPT and the scam emails at the touch of a button in "CEO Style"

Chat GPT is new, so the reported losses are not (yet) related to this AI application, even though it opens up completely new horizons for fraudsters: whereas previously they had to go through a relatively laborious process to gather the necessary information, for example by spying on the intranet, publicly available information in social networks or phishing calls at a wide variety of locations in the company, with ChatGPT there is a significant "optimization": The software is simply fed with data (e.g. employee letters, intranet content or email correspondence) and then spits out an email with a fake payment request in "CEO style". This raises the authenticity of the correspondence to a whole new level, and with it the chances that the "social engineers" will be successful.

Pressure factor: "Don't do anything wrong now"

But let's get away from the technical innovations, which do not pass by scammers either: Why does this scam work at all? Because it starts where we humans are touched at the core, where we have interfaces and (emotional) points of contact: Appreciation is a good example – or pressure. This can have many facets, such as time pressure, financial pressure, pressure to succeed, but also shame. Several "personal construction sites" at the same time, such as double workload in the home office with children at home, also quickly lead to overload and distraction and possibly avoidable mistakes under other circumstances. The pressure to please superiors can also play a role. Don't lose your job in these difficult times when inflation is through the roof and my credit is suddenly twice as expensive. In analogy to the "Fraud Triangle," pressure is certainly the dominant component in the fake president scam – please see also the article starting on page 8 and the interview with Mr. Schneider, Prof. PHD starting on page 14.

No security patch: Humans with their emotions remain the weak point

The human factor remains the weak point then- and every further advance in technology creates an even greater security gap. There is no simple security patch that can be applied to people.

Openness remains the most important factor against criminal machinations

Control and compliance systems play a rather subordinate role in social engineering cases – quite different to classic internal perpetrators. Nevertheless, there are ways and means that can easily put a stop to social engineers: openness, a good communication and error culture, and flat hierarchies. One call to the real boss is enough to expose the fraud immediately.

Critical questioning of employees, even in the case of urgent payment instructions, is essential, while acting "on autopilot" is dangerous. But managers themselves also have important tasks in prevention: This ranges from a sensible "tone from the top" and leadership qualities to a clearly communicated self-commitment not to issue transfer orders by telephone or video calls – and above all to stick to these rules.

> "Despite regular sensitization – the human being with his emotions remains the weak point.

Rüdiger Kirsch, Fraud expert and author of this article

How do perpetrators get caught?

Trust, but verify. Fraudsters are most often revealed by internal control systems, followed by whistleblowing. That´s why these two processes play a key role in prevention. Most fraud in companies is discovered by audits, other routine checks or by checking back on anomalies oddities. Other employees help too, with tip-offs and whistleblowing leading to a large percentage of internal criminals being caught. That's why protecting whistleblowers is increasingly important. Companies should think about internal channels and processes to protect those who come forward to report fraud or other crime. When fraudsters aren't revealed by internal audits or tip-offs from colleagues, perpetrators are often simply caught by pure chance. They get sloppy, make mistakes, or simply decide they can't live with fraud on their conscience and confess to the whole thing.

1. Internal processes

- **routine checks/ audits**
- **checks on anomalies**

2. Whistleblowing

- **tip-offs from other employees**
- **tip-offs from outsiders or collaborators**

3. Pure chance

4. Confessions

Source:
Allianz Trade Loss Statistics

The Law on Protecting Whistleblowers: What is it and what does it mean for companies?

The EU Whistleblower Protection Directive was introduced in 2019 and is to be implemented into every European legal system. This law intends to protect whistleblowers from all kinds of negative consequences. For most companies, public authorities and municipalities that means that they will be obliged to set up an internal whistleblowing system. Tip-offs from employees will thus be encouraged by law and court practice.

According to a study by the University of Applied Sciences of the Grisons, only 55 % of respondents had a notification officer in 2019. With the legal obligation and the new whistleblowing systems set up as a result, it is to be expected that significantly more anomalies will be reported and cases of wrongdoing by insiders detected.

In particular, cases such as the "hospital mafia" (see p.17), which pilfered stocks for 15 years without getting caught, should be detected much faster, since whistleblowers will be protected and will not, as in that case, have to likely face being sacked or suffer reprisals.

Lawyer Hendrik Schneider, Prof. PhD.
is a legal scholar and criminologist. In his research, he has dealt extensively with different perpetrator profiles as well as their motivations.

INTERVIEW

"The first time is often a pacemaker into crime"

What are the different types of perpetrators, how do they differ and why do they actually become perpetrators? Hendrik Schneider, Prof. PhD reports on the differences and motivations of white-collar criminals – and what companies can do to protect themselves from white-collar criminals right now, but especially in the future.

Allianz Trade is the trademark used to designate a range of services provided by Euler Hermes.

According to Allianz Trade loss statistics, the "typical perpetrators" who cause the most damage are highly educated men in their mid-40s, managers who have been with the company for at least 10 years; colleagues describe them as „conspicuously inconspicuous" up to now. Why?

White-collar criminals are "latecomers to crime", meaning late bloomers in their criminal career. There are several reasons for this. A graduate fresh from university, for example, would not have the authority to order transactions involving large sums of money. A manager with many years of service, on the other hand, knows how things work, where there are niches and control deficits, and has the necessary authority. Some people are tempted to take advantage of a favourable opportunity. This can be seen, for example, in the extreme increase in proceedings for subsidy fraud in the Corona crisis in 2020 by a staggering 2285% with losses of around EUR 95 million. However, no one in a position to apply for economic subsidies, for example, can get a clean police record. In other words, a clean slate is the basic prerequisite for white-collar offenders.

Why is it actually mainly men?

That's hard to say – one of the reasons is certainly that there are still more men in corresponding management positions.

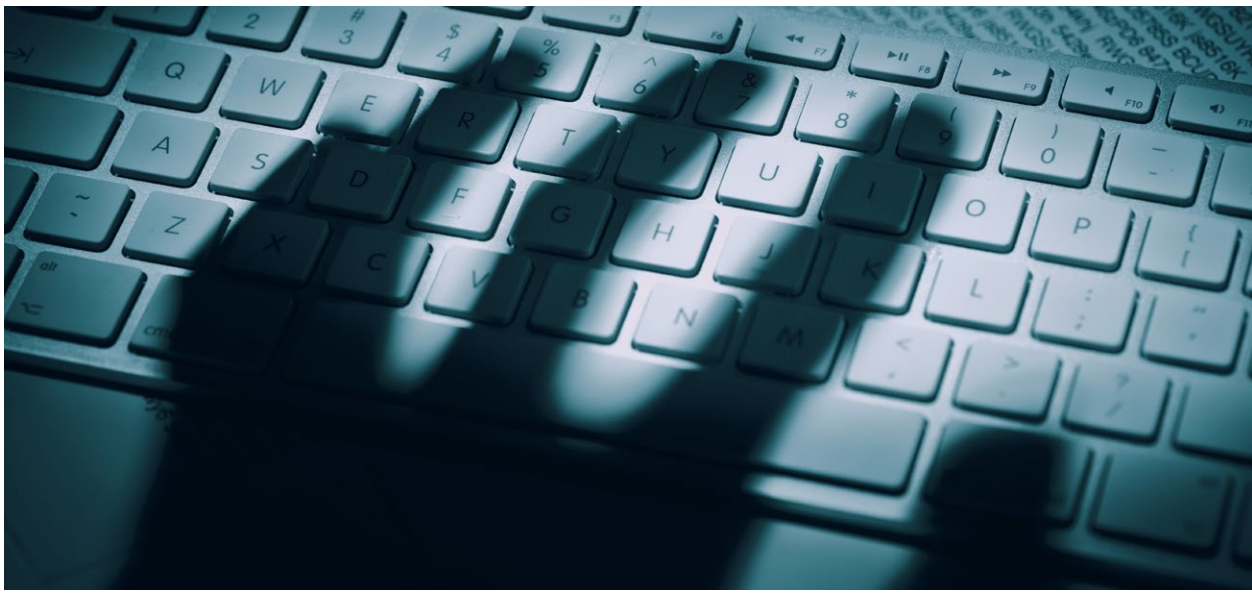
When we talk about "typical perpetrators," age, position and company affiliation say little about the perpetrator's personality. Are there any characteristic traits?

On the one hand, we differentiate between opportunity seekers and opportunity seizers. As the name suggests, some proactively look for vulnerabilities and others react to an opportunity that arises. There are also personal risk factors. We differentiate between four types of perpetrators: the perpetrator with economic criminological stress syndrome, the crisis perpetrator, the dependant and the inconspicuous one.

What drives them?

The dependant is – as the name suggests – usually an accomplice and henchman of a dominant main perpetrator on whom he is economically or hierarchically dependent.

The perpetrator with economic criminological stress syndrome, on the other hand, lives an unrestrained life at the moment according to the motto "earning and burning money" and is part of a "work-related subculture". Often the crimes occur in a biographical upheaval phase that is associated with control deficits and lack of involvement, e.g. the job abroad, divorce, etc. He is an opportunity seeker who immediately seizes every opportunity that comes his way.



Does opportunity actually make the thief?

Sometimes that actually is the only trigger. It's exactly the same with the "inconspicuous" person. This type of perpetrator actually has no or only very low personal risk factors. The temptation of the favourable opportunity was simply too great. If the crime comes to light, everyone around him is surprised because he was previously inconspicuous and conformed to the rules and would fall through the cracks in a risk screening.

Additional payments for electricity or heating costs, high inflation and rising interest rates are currently presenting many people with major problems. Do companies now have to fear crisis perpetrators and what makes them so?

In this respect, we are talking about economic pressure situations that are increasingly occurring under today's economic conditions. From the perpetrator's perspective, the crime may represent the only way out of the financial crisis. Because the act conflicts with his self-image, neutralization techniques help him to smooth out the inner turbulence, e.g. "I'm just borrowing the money"; "The insurance will compensate the loss anyway."

But not everyone becomes a criminal?

No. Crisis perpetrators are under massive pressure, but there are of course ways out that do not involve criminal offenses – in extreme cases, filing for bankruptcy. But not everyone is ready to take these steps or to adjust their living standards downwards during the crisis.

You mentioned neutralization strategies. How should we imagine such strategies?

White-collar criminals are not inherently immoral. Crisis perpetrators in particular often have high values and therefore have difficulty justifying criminal acts to themselves. "It's just this one time", "I'm just doing what everyone else is doing", "It doesn't affect anyone else personally, they can afford it" can be justifications like this.

If perpetrators still see the need to rationalize something, this is actually a good sign that all is not yet lost. This means that there is still a value orientation and inner turbulence that raises the alarm. But it could also be the beginning of the end.

When do they become repeat offenders?

The first time is either actually just a one-off – or a pacemaker into crime. The first time, the inhibition threshold is often high. But there is success learning and a habituation effect. The more often one lies or cheats, the lower the discomfort. At some point, the alarm bells no longer ring and it then runs virtually by itself. As long as the facade and camouflage are intact, perpetrators often don't even notice how criminal they are because this gradual slipping means that it doesn't feel so criminal at all - that often doesn't come until the court case. This is called a "drift into entrenched criminality," and white-collar criminal careers can develop.

Incidentally, this is also the case in workplace-related subcultures. In these parallel worlds, people are among like-minded people and there is no objective corrective. When, over a beer in the evening, you review how slyly you acted today, completely new value spaces are created and you are in harmony with your environment. The group dynamic means that they don't need neutralization techniques. However, it also leads to being pulled into the abyss even faster. Then, at some point, the rude awakening will come.

Speaking of a rude awakening: Aren't the perpetrators afraid of being discovered and losing their jobs?

In fact, the perpetrators – contrary to many assumptions – usually have a lot to lose. The risk of detection does play a role in their consideration of whether to succumb to the lure of the opportunity to commit the crime.

But there is often a big difference between the objective and the subjective risk of detection. Risks in the future that seem far away are often weighted less heavily.

If I, as the perpetrator, know that the deeds could be discovered during the next audit, it makes a difference for the subjective risk of discovery whether the next audit takes place in three weeks or in three years.

Keyword control systems – how can companies protect themselves?

Good control and compliance systems and clean processes are the be-all and end-all, because they minimize the opportunities for crime. At the same time, it is important to constantly think ab out the new risks that could arise in the future as a result of digitalization, increasing cyber-attacks, new technologies, and artificial intelligence such as ChatGPT. Fraud schemes are likely to accelerate just as rapidly as technological progress. When a fake boss can spit out a "CEO style" email at the push of a button, professionalism and scalability speed into new realms.

Indeed, this is also a generational issue. That's why it's important to have young, technology-s avvy employees on board who are aware of the risks involved. Incidentally, this applies to compliance as well as to supervisory boards.

You can also simply do a self-test and try it out. Send a chat GPT mail to your own organization. This will allow you to mercilessly identify your own weak points in processes and control mechanisms.

What role does corporate culture play?

The corporate and error culture as well as the "tone from the top" play an important role. Autocratic or very hierarchical cultures favour "breaking out" and are often much more susceptible to white-collar crime. As is often the case, balance makes the difference.

In some companies, complementary dual leadership can work well, and in fact diverse teams are helpful for both corporate culture and corporate success. When different points of view, perspectives and value orientations come together, things are questioned and considered in a completely different way. This often leads to a much more differentiated approach and helps with important decisions and culture.

The 4 perpetrator types and how they differ

THE PERPETRATOR WITH ECONOMIC CRIMINOLOGICAL STRESS SYNDROME

According to the competent criminal judge, the need for "unrestrained burning of money" was the driving force behind a case of top management fraud with a total loss in the double-digit million range. Being able to afford a lifestyle along the lines of "earning and burning money" with an unrestrained life in the moment is often the driving force of perpetrators with white-collar crime syndrome.

In the example case, the perpetrator afforded himself a yacht, custom-made furniture made of tropical hardw oods and consumed only particularly fine wines.

The clarification of the case impressively shows that a lack of controls, insufficient dual control principles, deficient compliance systems and an excess of control by the perpetrator over processes and subordinates represent a breeding ground that causes long-term victimization of the company w ith considerable financial losses. If these situational conditions are met by a perpetrator with, as the judge stated in the example case, "considerable criminal energy", considerable financial losses can arise, up to and including the insolvency of a medium-sized company.

Even after the acts of embezzlement became known, the perpetrator, who as a regular churchgoer and member of a "strictly Christian traditionalist fraternal movement" had put on an appropriate cloak of disguise, had done everything in his power to keep the fraudulently obtained funds. For example, he tried to thwart claims for damages by his former employer by making donations to third parties.

Allianz Trade is the trademark used to designate a range of services provided by Euler Hermes.

THE INCONSPICUOUS ONE

In a quantitatively significant number of constellations, no personal risk factors can be identified, but the act is explained solely by the presence of the favourable opportunity. Long company affiliation and deficient controls are characteristic for corresponding situational conditions. There may be a learning for the successful offender.

In one of the analysed example cases of Allianz Trade, the perpetrator had been the sole managing director of a wholesale company since 1991. After 20 years of service in an unchallenged management position, he decided to commit crimes of embezzlement to the detriment of the employer.

The acts were committed over a period of three years before they were discovered and an auditing company was commissioned to carry out an internal audit on the basis of identified irregularities. The offenses involved embezzlement. The perpetrator was involved in private luxury trips, some of which were taken with couples who were friends, as well as birthday parties abroad at company expense.

The perpetrator, who was not under economic pressure, could have financed the trips privately. It is possible that the arguments used by him in the trial, that it was a matter of "maintaining contacts" with future or current business partners and colleagues, also serve as justification in the form of neutralization strategies in order to smooth out the internal waves that were running high.

THE CRISIS PERPETRATOR

Crises can be economic crises or general life crises. In an example case with a conviction of the perpetrator in 2023, the perpetrator, a commercial employee, was under economic pressure because he had become addicted to online gambling.

When the possibility of obtaining funds for online gambling through legal means, such as loans, was exhausted, he took advantage of opportunities to commit crimes to the detriment of his employer.

Over a period of two years, he issued false invoices for work not performed. By doing so, he caused his employer, who assumed that the company indicated in the invoice had performed the work, to transfer a total of around EUR 500,000 to an account that was solely subject to the perpetrator's access. The acts involved forgery of documents and commercial fraud.

THE DEPENDANT

If more than one person is involved in the crime, the professional hierarchies are usually also reflected in the commission of the crime and the distribution of the loot.

In an example case from 2019, the perpetrator was employed in a managerial position at a company that either repaired or scrapped certain steel products on behalf of various customers.

The perpetrator managed to divert steel and temporarily store it in containers through certain manipulations. This material was then resold for cash. The main male perpetrator received support from a female branch manager, who finally confessed during the police investigation. The branch manager was responsible in particular for collecting the cash and received a share of 10 %. She had to pay the difference to the main perpetrator, who used the money mainly for the purchase of luxury cars and a "city villa with two garages and adjoining rooms".

How can companies protect themselves from black sheep?

Fraud and embezzlement remain in the top 3 offenses in the area of white-collar crime. 36% of affected companies in Germany recorded losses due to fraud in 2022. Only theft and asset misappropriation (39%) as well as data theft and data abuse (38%) were even more common*. There are more black sheep than many companies think, and they cause huge financial losses year after year.

In most cases they are very hard to identify. They often blend in so well that the most suspicious thing about them is how un-suspicious they are. They're friendly, fit in well and are completely integrated with your team. In fact, many of the qualities you'll look for in a good, high-achieving worker are also the qualities that make a successful fraudster – such as determination to succeed, an appetite for risk, ambition and a focus on getting to the top.

That's why it's so important for companies to find the right balance between trust and corporate culture on the one side and prevention and control on the other.

Satisfied employees who feel comfortable are respected and appreciated by their managers and colleagues and happy with their roles, pay, prospects and personal development are normally far more loyal than those who find themselves in a toxic working atmosphere.

Harassment, frustration and revenge are often the motives which prompt insiders to commit crimes. That means a welcoming, tolerant corporate culture and transparent communication are vital in keeping your employees on your side. When people who work together trust each other and feel comfortable raising problems, weak points can be identified, loopholes closed and criminals identified much faster. But it's not all about being friendly. Control mechanisms, guidelines and regular routine checks are just as important for your company's protection, because it's often opportunity which creates thieves.

Despite all those checks, bad apples always find ways and means to commit fraud.

Most inside criminals have a criminal mindset and a degree of ingenuity that helps them seize opportunities as soon as they present themselves. They're even able to get around the best control processes.

That's why you can never become complacent about the processes you have in place or become lulled into a false sense of security. You should always take extra steps to protect yourself, by finding expert advice and by making sure you're covered by comprehensive business fraud protection.

**Source:*
KMPG, Study White-collar crime in Germany 2023

Allianz Trade is the trademark used to designate a range of services provided by Euler Hermes.

Trust & Culture

An open, trust-based **corporate culture** with flat hierarchies

A good, constructive **culture of criticism of errors** and open communication

Clearly formulated **corporate guidelines and ethical** values which are also integrated into day-to-day work

A cooperative, democratic **leadership style,** appreciation, trust and respect

Good **working conditions:** fair pay, financial incentives, rewards for performance, interesting challenges

Equal opportunities, diversity, fair career prospects with clearly defined, objective and transparent criteria

Talent management and development; further training in hard and soft skills and promotion of young talents

Satisfaction surveys of staff; Implementation of measures to increase staff satisfaction levels

Support for employees in (personal or financial) difficulties through appropriate assistance or counselling programmes

Precautions & Controls

Putting **control and Compliance systems** in place; in particular the separation of functions (4 or more eyes principle)

Campaigns and training to raise awareness in staff for **internal guidelines** and critical situations and **how to detect anomalies**

Regular **routine checks,** internal audits, where needed checks by external third parties

Implementation of secure internal (and where appropriate, external) **whistleblowing channels** (e.g. ombudspersons) and regular information to staff

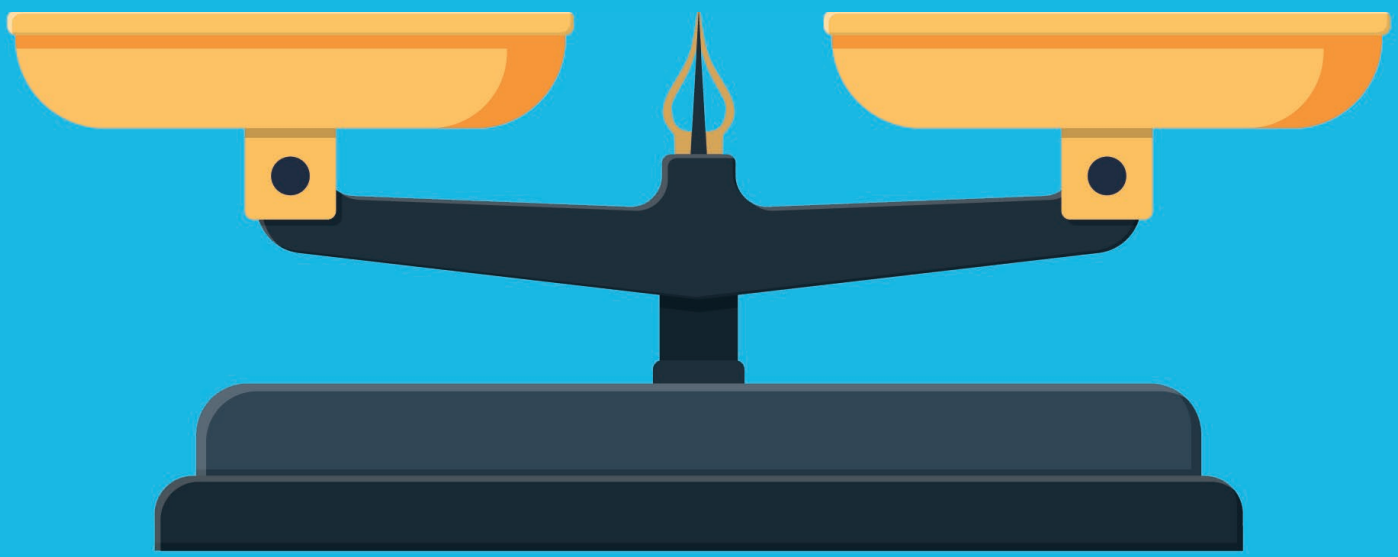
Preventive risk management and regular process optimization: review and improvement of possible system vulnerabilities incl. authorization and access controls

Vigilance and **observation to notice any irregularities,** e.g. anomalies in working hours, attempts to access restricted data or the use of unauthorized data media

Immediate, transparent and objective investigation in the event of suspicion

Checks on job applicants, e.g. compliance screening, police clearance certificate, Schufa report, plausibility or background checks, references

For especially security-sensitive positions where appropriate **determination of personal factors,** e.g. Hannoversche Corruption Perceptions Index



Close the loopholes

Sometimes you can do everything right and still fall victim to fraud. You can take all the right precautions, and fraudsters will still find a tiny gap to squeeze through. But that doesn't mean you shouldn't effectively and systematically close every security loophole you find. The best way to do that is to regularly check all the **most common risk factors** and act accordingly.

1. Corporate Structure Risks

- **a.** Are workflow and processes in the company clearly demarcated?
- **b.** Are there people in the company who are responsible for keeping themselves updated on necessary and potential security measures?
- **c.** Are there emergency plans in place for security breaches?

2. Recruitment Risks

- **a.** Do you investigate unusual notice dates or frequent job changes when vetting an applicant?
- **b.** Do you carry out additional checks on candidates for key positions (references)?
- **c.** Do all employees need to sign a declaration of confidentiality regarding company internal matters?
- **d.** Does the management have a crisis scenario for business fraud losses?

3. Data and IT Risks

- **a.** Do you have IT security systems and processes?
- **b.** Is data classified according to sensitivity and have appropriate protections been implemented?
- **c.** Is your IT protected against attacks from outside?
- **d.** Are passwords regularly changed?
- **e.** Do you have unsecured internet connections in the company?
- **f.** Are your online connections to your bank properly protected?

4. Payment and Transfer Risks

- **a.** Are the accounts department and the cash desk strictly separated?
- **b.** Are cheque forms kept locked away and are serial number ranges checked?
- **c.** Do you use facsimile signatures in your company?
- **d.** Are preventive controls in place?

5. Postal Risks

- **a.** Is incoming post registered with a date stamp?
- **b.** Are incoming cheques logged and recorded?

6. Sales and Purchasing Risks

- **a.** Are different people responsible for:
  - placing orders,
  - registering incoming goods,
  - authorising payment for goods?
- **b.** Are inventory checks of goods in stock carried out regularly?
- **c.** Are returned goods recorded separately?
- **d.** Does the company have a code of conduct for purchasers?

7. Internal Audit and Control Risks

- **a.** Do you have your own internal audit department?
- **b.** Do they or an external auditor carry out regular audits on all departments of the company?
- **c.** Is the 4-eyes principle applied consistently throughout the company? And how does it work, for instance, if people work from home?

Allianz Trade is the trademark used to designate a range of services provided by Euler Hermes.

Allianz

Allianz
Trade

I have full confidence in
my employees
are a risk factor for the company

Protect your company against the consequences of business fraud:

ALLIANZ-TRADE.DE/VERTRAUEN

Well equipped against risks

Protect your company against financial losses through wilful unlawful acts by insured persons and certain third parties.
Any questions for us?
Whether you're already a customer or not, we'll be delighted to help.

Phone + 49 (0) 40 / 88 34 - 35 36
service.de@allianz-trade.com
www.allianz-trade.de/vertrauen

Euler Hermes Deutschland
Niederlassung der Euler Hermes SA
22746 Hamburg
Phone +49 (0) 40 / 88 34 - 0
Fax +49 (0) 40 / 88 34 - 77 44
info.de@allianz-trade.com
www.allianz-trade.de

05 7000e 1123

Allianz Trade is the trademark used to designate a range of services provided by Euler Hermes.