A World Apart? Private Investigations in the Corporate Sector

Clarissa Meerts*

Abstract

This article explores the investigative methods used by corporate security within organisations concerned about property misappropriation by their own staff and/or others. The research methods are qualitative: interviews, observations and case studies carried out between October 2012 and November 2015. The findings include that, even though corporate investigators do not have the formal investigative powers enjoyed by police and other public agencies, they do have multiple methods of investigation at their disposal, some of which are less used by public investigative agencies, for example the in-depth investigation of internal systems. Corporate investigators also rely heavily on interviews, the investigation of documentation and financial administration and the investigation of communication devices and open sources. However, there are many additional sources of information (for example, site visits or observations), which might be available to corporate investigators. The influences from people from different backgrounds, most notably (forensic) accountants, (former) police officers, private investigators and lawyers, together with the creativity that is necessary (and possible) when working without formal investigative powers, make corporate security a diverse field. It is argued that these factors contribute to a differentiation between public and private actors in the field of corporate security.

Keywords: Corporate security, private investigations, private troubles, public/private differentiation

1 Introduction

> I remember from my time in the police that we were always complaining that private investigators were able to do anything and could just barge in somewhere. And now that I'm on the private end we as private investigators complain that we *can't* go in because we don't have the authority to do so. If someone doesn't want to cooperate we can't do much. [Respondent 5]

Many concerns have been raised about the existence of a private market for security; however, much less attention has been given to the actual activities of this field.[1] As the quote above shows, a recurrent image of private investigators is that they have much leeway and are not bound by rules or moral considerations in their investigations. Interestingly, private investigators, on the other hand, often feel restricted because they do not have the legal investigative powers law enforcement agencies are endowed with. Our knowledge about the large (and growing) involvement of private actors in the field of security provision is still somewhat behind the curve and merits more extensive scientific attention.[2] One of the relatively under-researched parts of the private security industry is what will be called 'corporate security' in this article. Although there is little recent work on the corporate security industry in its entirety, earlier work has been done on its specific parts.[3] The article aims to provide insight into private corporate investigations. This focus on the investigations instead of a specific kind of investigator (for example forensic accountants) makes for a more encompassing understanding of the field. The commonalities between these various investigators warrant such an approach, in spite of the differences between them. The recent emergence of forensic departments in law firms, and developments in investigative methods (e.g. with regard to IT tools used for investigations) furthermore indicate that the sector is one in development, making it interesting to take a closer look at the sector as a whole. A good understanding of the activities of the sector will facilitate a solid discussion on the positives and negatives of the corporate investigations industry.

The article explores the corporate security industry by focusing on private, corporate investigations into behav-

* Clarissa Meerts, MSc., is a PhD student at the Criminology Department of the Erasmus University Rotterdam. This research was made possible by funding by the NWO MaGW Research Talent 2011 grant (the Netherlands Organisation for Scientific Research, Division of Social Sciences) and by the assistance of anonymous interviewees and participants in the observations. The author would, furthermore, like to thank Nicholas Dorn, Sanne Taekema and anonymous reviewers for their useful comments on earlier drafts of this article.

1. *See*, for example, the report of KRO Brandpunt, 'Bespied door de baas' (1 June 2014). Available at <http://brandpunt.kro.nl/seizoenen/2014/afleveringen/01-06-2014>.
2. K. Walby and R. Lippert (eds.), *Corporate Security in the 21st Century: Theory and Practice in International Perspective* (2014).
3. On the different parts of the industry, there is some interesting work available. *See*, for example, J.W. Williams, 'Reflections on the Private versus Public Policing of Economic Crime', 45 *British Journal of Criminology* 316 (2005). M. Gill and J. Hart, 'Exploring Investigative Policing: A Study of Private Detectives in Britain', 37 *British Journal of Criminology* 549 (1997). M. Nalla and M. Morash, 'Assessing the Scope of Corporate Security: Common Practices and Relationships with Other Business Functions', 15 *Security Journal* 7 (2002).

iour by firms' staff, management, subsidiaries and subcontractors that is considered problematic by these firms. The greater part of 'incidents' occurring within organisations never reaches the criminal justice system, and it is important to take a closer look at the actions of these corporate investigators.[4] These incidents may concern (alleged) criminal behaviour such as fraud, but they may just as well be about behaviour that is considered undesirable rather than criminal, for example conflicts of interests. Although all kinds of unwanted behaviour may be investigated by corporate investigators, most incidents have an economic background (theft, fraud, favouritism in the granting of contracts, etc.). Working outside the formal investigative powers of public law enforcement agencies, corporate investigators operate in ways tailored to the problems that concern their clients. The services provided by corporate security investigators include, for example, forensic accountancy, (private) investigations more generally, IT services, asset tracing, drafting and implementing integrity codes and (assistance with) settlement and prevention tactics.[5]

'Corporate security' is a broad term that contains all actors that are involved in the investigation of incidents within organisations (consisting of economic loss, misappropriation of assets, reputational issues and the like). The field is quite diverse and includes private investigators, forensic accountants, in-house security departments and lawyers. Clients of corporate security may be both commercial and (semi-)public organisations. Respondents indicate that most of their clients are medium- to large-scale companies, which they attribute to the costs of investigations. In this article the term 'client' is used to indicate the consumers of corporate security services. In the case of an in-house corporate security department, the client is for example the company's management.

Some corporate investigative methods are broadly similar to those used in public policing (e.g. interviewing the people involved or observing someone – although the degree of duress, rights of the interviewee, etc. may differ), whereas other investigative methods are more private in origin and in 'ownership' (e.g. forensic accounting methods or an audit of internal systems). Corporate investigators have the same investigative powers as any citizen, which means in practice that they can operate with considerable flexibility.[6] Depending on their professional background, investigators may or may not need a permit under Dutch law (the Wpbr). The Wpbr only applies to private investigation firms, excluding in-house departments (not working for a third party), forensic accountants and lawyers (as they have their own (but general) regulations). The Dutch regulation of corporate investigations is thus rather scattered. The Privacy code of conduct, obligatory to Wpbr- permit holders seems to be followed by most respondents, though. In addition, more general laws such as the criminal code and privacy legislation (the WBP) apply to all investigators.

Many rights and possibilities of corporate investigators are derived from the rights the client has as an employer.[7] In broad terms, employers are allowed to exercise control over their employees; however, they should take certain restrictions into account. In general, principles such as legitimacy, subsidiarity, proportionality and the right to privacy apply. When corporate investigators investigate a case, they might gather a great deal of information by talking to people (interviewing), by looking into internal systems (e.g. personnel logs), firms' communications (email, phone records), financial systems (accounting, sales and other systems) and open sources (e.g. social networks) and by tracing assets. Crucially, in terms of access and speed, there is no need for them to wait for the approval of a prosecutor or judge prior to the use of these methods – corporate investigators merely need approval by the client/management. On the other hand, it is impossible for corporate investigators to, for example, lay claim to financial records of *other* firms, or to enter other premises – these being powers granted exclusively to public law enforcement. This may mean that it proves impossible for corporate investigators to investigate an incident fully. Many corporate investigators have a background in law enforcement. One frequently mentioned reason for this career switch is the perceived bureaucracy of the state apparatus and the expected freedom private investigators enjoy. However, corporate private investigators, on their part, feel that they are limited in their possibilities as well, as they lack formal investigative powers. When formal powers of investigation are necessary for a full investigation, law enforcement agencies have to get involved. Whether or not police and prosecution are mobilised by a report to the police depends on the client. This decision might be influenced by some advice provided by corporate investigators, although some investigators refrain from giving advice.

In this article the focus is on investigations into incidents within organisations. How do corporate investigators conduct their investigations and what kind of methods of investigation and sources of information do they have at their disposal? Clients rely on investigators to provide them with the information they need to react to the incident at hand – it is interesting to take a closer look at the ways this information is gathered. In the article the investigative process is considered, from the moment an incident is reported to the investigators to the moment investigators report their findings. The discussion reflects upon the material presented in this arti-

4. N. Dorn and C. Meerts, 'Corporate Security and Private Settlement: An Informal Economy of Justice', in J. Shapland and P. Ponsaers (eds.), *The Informal Economy and Connections with Organised Crime: The Impact of National Social and Economic Policies* (2009) 113.
5. Williams (2005), above n. 3; C. Meerts, 'Corporate Security – Private Justice? (Un)settling Employer-Employee Troubles', 26 *Security Journal* 264 (2013).
6. Williams (2005), above n. 3.
7. J.W. Williams, 'The Private Eyes of Corporate Culture: The Forensic Accounting and Corporate Investigation Industry and the Production of Corporate Financial Security', in K. Walby and R. Lippert (eds.), *Corporate Security in the 21st Century: Theory and Practice in International Perspective* (2014) 56.

cle, arguing that the field of corporate security is characterised by a double differentiation – both externally (from law enforcement) and internally (within the corporate security field).

1.1 Methodology

This article is based on qualitative data gathered between October 2012 and November 2015, as part of a PhD research, funded by a NWO Research Talent grant. An important source of information for the research consists of fifty-four semi-structured interviews that have been conducted with corporate investigators (thirty), clients (ten) and law enforcement professionals (fourteen).[8] Respondents were approached through snowball sampling and gatekeepers, making use of previous contacts and previous research by the current author. Snowball sampling has proven an effective way to reach respondents in a 'hidden' setting.[9] Although corporate investigators themselves are not hidden, and indeed sometimes advertise their services, there is no clear overview of how many corporate investigators there are in the Netherlands – partly because only those who call themselves private investigation firms officially require a permit. Clients highly value the discretion applied by corporate investigators and as such, many investigations remain private. Clients are therefore difficult to reach without referral by a gatekeeper. Because many investigations remain out of sight of the criminal justice system, finding law enforcement professionals with knowledge on the subject is equally challenging without a gatekeeper. Referral by a trusted gatekeeper furthermore has the added benefit that participants tend to trust the interviewer more easily, which may lead to more accurate data. To mitigate the problem of selectivity, multiple gatekeepers and starting points for snowballing have been used. At later stages of the research, saturation of respondents occurred, which is an indication that important respondents have been reached. However, a snowball sample is inevitably a purposive selection.

For each group of respondents a slightly modified topic list was used, so as to take full advantage of the knowledge of the respondent. Topics included regulation, private investigation methods, private settlement decisions and relationships between public and private investigators. Interviews had an average duration of one hour and twelve minutes, with the shortest interview spanning twenty-six minutes and the longest two hours and fifteen minutes. All interviews were conducted face-to-face, and most interviews were with a single person, although a few were conducted with two respondents at a time. When possible, the interviews were recorded to be transcribed verbatim at a later time. One respondent did not consent to being tape-recorded,[10] and on eight occasions it was not practical to record the conversation; in these cases extensive notes were taken.

In addition, two observations were conducted, one with an independent corporate security firm (end of 2012, seven weeks) and one with an in-house corporate security department within a large Dutch firm (early 2015, six weeks). The two different settings were chosen to see whether the general picture of corporate investigations would be similar in the different contexts. From these observations, rich data has been derived. The observations were recorded in a daily observation report, based on an observation schedule. During the observations both informal conversations and interviews were conducted.[11] In addition, the observations provided twenty-one case studies, which were separate case files from investigations done by the observed investigators. Cases were selected on the basis of criteria such as employee involvement, sensitivity of the incident, the type of settlement chosen and the involvement of law enforcement. They were analysed using a topic list, describing, among other things, the case, the (type of) client, the investigative methods, the interests that were involved, the settlements chosen and the role (if any) of law enforcement. Not all information could be gathered from the case files; however, additional questions to the investigators often provided an answer here.

All data gathered is treated with utmost confidentiality and has been anonymised to ensure that no information can be traced back to the respondent or his or her employer. The article should not be regarded as generalising to the Netherlands as a whole; the statements made are indicative of the respondents in the research (who do suggest that their statements are more generally applicable).

2 The Appeal of Private Investigations

In the Netherlands, as in many other countries, private parties do not have legally defined powers of investigation. This circumstance means corporate investigators are restricted in their investigations as they are not allowed to, for example, enter or search premises without the consent of the owner. This type of far-reaching investigative power is reserved for law enforcement and safeguarded by legal norms.[12] On the other hand, not

8. The respondents are not equally divided among the three groups. The reason for this lies partly in the fact that the research project is ongoing and not all data had been gathered at the time of writing. In addition, the choice was made to put emphasis on the investigators. Saturation was achieved. Care was taken that the selection of respondents reflected the Dutch situation. For example, among the group investigators, respondents were selected from private investigative firms, in-house security departments, forensic accountancy departments and law firms.
9. M. Lamont and P. White, *Report on Workshop on Interdisciplinary Standards for Systematic Qualitative Research: Cultural Anthropology, Law and Social Science, Political Science, and Sociology Programs* (2014).
10. The reason given for this was that the respondent felt she could not guarantee anonymity to her clients if the conversation was recorded. The respondent seemed to talk freely once she was assured of anonymity and that the conversation was only recorded through notes.
11. These formal interviews (four in observation 1 and seven in observation 2) are included in the total number of interviews mentioned above.
12. *See* the Dutch Criminal Code.

being endowed with investigative powers also means that the strict regulations and procedures a criminal investigation has to follow are not applicable to a private investigation. This gives the investigators considerable leeway to act within their means as they see fit. Private persons are allowed to investigate behaviour that is harmful to them – or to ask other private persons to do so – as long as they do not violate any laws. Legal persons are considered private persons in this sense, and when they act as client to corporate investigators, corporate investigators may use the investigative possibilities of their client. As an employer, a company has the right to control certain behaviours of its employees, and many companies have made provisions in the labour contract for the use of this information for investigative purposes.[13] Corporate investigators thus often have access to a lot of information.

Because of the large diversity of actors with different backgrounds working in this field – ranging from former police officers to lawyers, IT specialists and forensic accountants – there is a wide variety of skills and expertise, going well beyond those of police investigations. These skills are applied to provide clients with swift results that can be used to prevent future incidents and, possibly, restore at least some of the damage done. The different backgrounds of corporate investigators also mean that different rules and regulations apply. As mentioned above, specific legal regulations with regard to private investigations are provided only for Wpbr-permit holders (private investigation firms). For forensic accountants and lawyers working as investigators, there are the more general rules and disciplinary proceedings in place for their profession as a whole (additionally, in forensic accountancy there are principles of law expressed in (non-binding) guidelines). In-house investigators are governed by internal regulations. All investigators have to adhere to the law on the protection of personal data (WBP), and most respondents state they apply themselves to the more stringent principles of law applicable to accountants[14] and the privacy code[15] that has been written by the representative organisation of private security firms (which has been approved by the data protection authority). It would go beyond the scope of this article to discuss these different rules and regulations in depth, but where applicable, they are mentioned. It should be noted, however, that most rules regulating corporate investigators' behaviour remain very general. The Privacy code of conduct for Wpbr-permit holders is the most specific set of rules; however even these do not give guidance in every situation.[16]

13. C.D. Schaap, *De private forensisch fraudedeskundige. Een feitelijke en juridische positionering* (2008).
14. NIVRA/NOvAA, *NBA-handreiking 1122. Praktijkhandleiding persoonsgerichte onderzoeken voor accountants-administratieconsulenten/registeraccountants* (2010).
15. Nederlandse Veiligheidsbranche (NVB), *Privacygedragscode sector particuliere onderzoeksbureaus van de Nederlandse Veiligheidsbranche* (2016).
16. *Ibid*.

The diversity in backgrounds and accompanying expertise make the corporate security field of interest to prospective clients. In his work on forensic accounting and corporate investigations, James Williams has pointed out certain advantages of corporate investigations from the viewpoint of clients.[17] The flexibility in investigative methods and solutions; the orientation on private troubles rather than criminal acts; and the possibility of discretion and control are important characteristics that lead clients to prefer a corporate investigation over the involvement of law enforcement agencies. This indicates that distinctions between public and private remain relevant in the field of corporate security even though integrated networks of security seem to emerge in other areas such as public spaces or shopping areas.[18]

The article takes a closer look at the types of investigative methods and sources of information which make it possible to provide clients with the services and information they need. While corporate investigators stress their professionalism and neutrality, it is the client and its interests that are leading. Investigations are directed towards answering the questions that have been formulated in the assignment by the client. Thus, the services that are provided are tailor-made to meet the needs of the client. For example, when investigating a suspicion of fraud, corporate security investigators can be very cautious in their investigations, so as not to create unrest within the company. The interests of the client are prioritised in the investigations and this may mean that the investigations need to take a more subtle approach than the police would take.

> Ok so the police come in, take the administration. Do you have any idea what that does to an organisation? People go home sick, totally lost. And with us, things go more quietly. They don't even notice. They do when we start interviewing and that will produce unrest of course but that's at the end of the investigations. What we do is more subtle, we do custom made work. [Respondent 1]

Investigative firms and departments differ in their backgrounds and structure, as reflected by the observations conducted during this research. For example, there are large and small investigations bureaus (or forensic departments within accountancy or legal firms), and there are large and small in-house departments within large companies. Observation 1 was within an independent corporate security company, with six employees at the time of observation, of whom five were involved in (all kinds of) investigative activities. Observation 2 was within an in-house security department within a large Dutch company, with fifteen employees at the time, of whom eleven were involved in investigative activities. In Observation 2, there was a division of labour, with one team being responsible for the intake and registration of cases, one team focusing primarily on desk research and

17. Williams (2005), above n. 3.
18. Williams (2014), above n. 7.

one team (in the lead of the investigations) focusing on interviewing.

3 The Ambit and Language of Corporate Investigations

Depending on the position of the investigators, an investigation usually starts with an intake of the assignment (in the case of an external investigator) or the report of an incident to the security department (in the case of an in-house department).[19] In both cases it is customary that the 'owner of the problem' – be that the manager of the suspected employee, the Board of Directors or someone else – and the investigators talk about the reported incident in order to have a clear idea of the scope of the problem. The extent to which this is possible at the start of an investigation may differ widely. Respondents indicate that investigations may start with a very clear suspicion towards one person or a pretty straightforward problem, but it is also possible that the question put to the investigators is very broad. It happens, for example, that the client is merely aware that something is not quite right, but cannot put his finger on the actual issue. This means that the assignment of corporate investigators may be very specific or pretty broad. Respondents state that the goal is to define the assignment as strictly as possible before starting with the investigations. This is especially relevant for investigations conducted by external firms (as distinct from in-house or self-investigations) and in cases in which a certain individual is investigated (person-oriented investigations).[20] While this predetermined focus is helpful and beneficial to involved persons in the sense of the protection of their privacy, it also has the danger of the investigations being pushed in a certain direction. 'So carefulness and clarity are important in your investigations, making sure you are not being used as the stick to beat the dog and the individual is treated fairly' [Respondent 27].

However narrow an investigation may be at the start, during the investigative process the scope of the assignment may, in consultation with the client, be broadened or narrowed down. A broader scope usually means more investigations and thus more expenses, which makes deliberation with the client necessary. Respondents from in-house investigative units indicate they have more independence in determining the scope of the investigations. According to respondents, the dialogue with the 'problem owner' is especially relevant in the first phase of the investigations.

> [The level of contact with the client] depends on the phase your investigations are in, the nature of the issues involved. In the beginning of the investigations you're going to have much more contact with the client about things like, what kind of information are you going to need, what's available internally, which information will need to be secured right away… That's contact on the operational level, with the IT-department, the business line, the department that's responsible for the issue. And the question is for example, will it be necessary to collect your information quietly or do the employees already know there's going to be an investigation and is it ok for you to contact the department and deliberate? How are we going to secure the information, is it a lot, are we going to gather everything, digitalise the information and put it in a big computer so we can search efficiently later on? Or is it limited in scale and maybe already digitally present? Well, those are the kinds of questions that are relevant at the start of your investigations. [Respondent 13]

After the assignment is determined and the problem defined, the investigations can commence. The methods to be used depend on the case. The use of cameras may be very helpful to see who has taken money from a cash register, but it might prove useless in case of loss of money through digital channels. In addition, the internal information and systems that are available partly determine the path the investigations will take. Some clients may have their own camera systems, track-and-trace devices or other useful tools for investigations, while others do not. In some cases, an employee suspected of wrongdoing is kept in place purposively so investigators might catch him or her in the act. In others, the employee is suspended from active duty at an early stage of the investigations so he or she may cause no further harm. This also depends on the severity of the matter.

> With someone who has an important position in the organisation you don't want to wait until you have the results of the investigations before you act, he will be suspended immediately. That person will therefore know about the investigations in advance. When it's about the disappearance of items from the work floor or someone taking money from the till, you can wait and see what happens if you for example would mark a certain item [CM: to see who takes it]. There's much less of a rush there and the critical risk is less prominent. [Respondent 50]

In general, corporate investigators prefer a suspension over an immediate dismissal of the involved person for the duration of the investigations. 'Sometimes the circumstances warrant immediate action. We prefer a suspension [CM: over a dismissal]. So they are still held to comply with your investigations because of their labour relation with the client' [Respondent 1].

The order in which the various methods are used may differ. However, it is common to start with the investigation of administration and the interviewing of witnesses. The interview of the involved person(s) is usually reserved for the end of the investigations, so as to be

19. *Ibid*.
20. As distinct from broader investigations into the organisation, not focusing on an individual but an issue.

able to confront the person with the evidence against him or her. During the investigations, many corporate investigators keep an investigative journal for internal use. This journal records relevant actions taken by the investigators, contacts they may have had with people and other relevant information. Especially when there are multiple investigators involved in a case, this may prove very useful (however, respondents also indicate that the thoroughness with which this journal is kept differs among investigators). The journal can be regarded as a log and may be used for the eventual report.

After the investigations have been concluded, a draft report is made. Relevant parts of the report are then usually handed to the involved person to read, in accordance with the adversarial principle (see paragraph 6 of this article). After all involved persons have had the opportunity to exercise their right of inspection, the draft report is finalised and given to the client.[21]

As do most professional procedures, private investigations have their own language. In legal terms, the public and private activities are separated by different terminology. During my interviews and observations, most respondents from the private sector referred to their activities with different words than commonly used for criminal justice investigations, and some made a point of avoiding 'law enforcement terminology'. Interestingly, clients and law enforcement respondents seem to make less of an issue of this. However, most respondents avoid, for example, the word 'suspect', using the words 'subject' or 'involved person' instead.[22] The same goes for the information source of personal communication: private investigators do not *interrogate* but they *interview*.[23] This difference in terminology also emphasises the difference in investigative powers, as the power to interrogate someone is exclusive to law enforcement agencies. The Privacy code of conduct of the representative organisation of private security in the Netherlands (NVB) states:[24]

> This code of conduct abstains from the use of concepts that are present in the criminal code to avoid confusion with the detection of crimes by law enforcement agencies. Private investigations do not take place under the authority and responsibility of the public prosecution office after all, and furthermore, its goals are different.

The differences in terminology seem to separate private investigators and law enforcement on a symbolic level, something that respondents seem to confirm. As one of the investigators in one of the observations said, 'I'm no private police'. Even though there are many corporate investigators with a law enforcement background, and their work may seem similar to the work of police and prosecution, there are notable differences. In what follows, the principal components of a private corporate investigation are discussed. First, the various sources of information, leading up to the eventual confrontation in the interview, are explored. Paragraph 5 discusses the next step in the investigations, in which the involved person is confronted with the information that has been gathered. Finally, paragraph 6 examines the investigative report, which concludes the investigative process.

4 Gathering Information: Investigative Methods Leading up to Confrontation

4.1 Internal Documentation

An important source of information for corporate investigators is 'the paperwork'. 'It's difficult to assess whether the person is telling the truth and by starting with the financials, you can get a sense of what might have happened' [Respondent 5]. When business is conducted, actions are documented. This (digital or) paper trail is a very valuable source of information in the reconstruction of where the money went. Since the client usually is the organisation where the irregularities occurred, its records are generally available to the investigators. Because the client can order its employees to cooperate fully with the investigations, relevant parts of the organisation may deliver documented information quickly. These documents include 'anything that has been written down'. 'We usually start with the records. And that is a very broad concept of course. There are financial records, digital but also hard copy. Digital is for example the books and hard copy the invoices, source documents, everything that the books are based on' [Respondent 5].

The way these documents are constructed depends on the type of services or products the client delivers, but generally there are invoices, contracts, tenders and project reports available. These source documents may provide an overview of what happened fairly quickly.

> That provides you with a lot of information, transactions are documented of course. There is someone ordering, there is someone who approves it, there is someone who enters it into the system.… Payments are usually cashless, which means there are bank records of them. So you try to gather all relevant information, refine your knowledge and document it. [Respondent 28]

Much can be derived from the financial administration of an organisation. Sometimes this provides a straight-

21. J. van Wijk, W. Huisman, T. Feuth & H.G. van de Bunt, *Op deugdelijke grondslag; een explorerende studie naar de private forensische accountancy* (2002).
22. This article also avoids 'criminal law terminology', as the use of these terms would be incorrect in this context. An involved person, for example, is not a suspect in the sense of a criminal procedure (and as such does not enjoy the same rights). The adversarial principle could be interpreted as being a criminal justice term (as it is a leading principle in criminal proceedings); however, in the Dutch legal system, this is a term that is used in all legal proceedings, from administrative to civil to criminal, and is thus not specifically linked to the criminal justice system.
23. *See* for example NVB, above n. 15.
24. *Ibid*.

forward story and not much additional investigating is necessary. Outgoing payments from the accounts of the client often provide information on the person who received the money. However, there are situations where constructions are used to disguise the path the money has taken and to hide the recipient. Information provided by the client might not be enough to trace the money or find out what happened. The access to documentation is limited to internal information from the client, although involved persons may (and sometimes do) provide access to their personal accounts. Sometimes this means that – because of the lack of investigative powers – corporate investigators will not be able to pinpoint the problem. 'There are situations where you need the powers of investigation of the police. Especially in these financial investigations. Sometimes you need a warrant to get bank records. We can't get to bank records of third parties – that would be highly illegal' [Respondent 1]. This problem of access makes it more difficult for corporate investigators to investigate the incident fully when, for example, subcontractors are involved. 'In the big investigation I told you about, there was a subcontractor involved and he had his administration, probably, at home. It wasn't available at our client company so we figured he kept it at home. We asked him for it but he didn't give it to us of course' [Respondent 5].

4.2 Internal Systems

There are many different 'internal systems' an organisation may use. Generally speaking, all these internal systems may be put to use for an internal investigation, as long as certain requirements are met (e.g. the employer has to announce in general terms to his employees that their movements may be tracked). Most of these systems are not meant for investigative purposes but can be used anyway. What kind of system is available depends largely on the (economic) activities of a client company. For example, logistics companies often have track-and-trace systems in their vehicles, and security cameras are used more often in a large warehouse than on an office floor.

4.2.1 Communications and Data Carriers

One category of internal systems revolves around employees' communications and use of data carriers. Email-inboxes, mobile phones, PC's, laptops and USB sticks may be searched when they are owned by the employer.[25] This means that investigators are allowed to investigate the use of company facilities. There are multiple, more and less intrusive ways to investigate communications and data carriers. According to the widely used principles of proportionality and subsidiarity, investigative methods should be proportional to the goal (and the interest of the client in reaching this goal) (proportionality), and the least intrusive methods should be used when possible (subsidiarity). For example, one could use a phone tap to record a telephone conversation, but one could also use mediation to track a phone. Mediation and inspection of phone bills are less intrusive because while they show where the phone has been and who has (been) called, the content of the conversation is not recorded. Often, mediation is a very useful tool. For example, in one of the cases used for the case studies, mediation was used to prove that an employee was near the building where some equipment was stolen on the day of the theft, even though he had called in sick and was no longer working in the building.

When, for example, some property has gone missing it might be helpful to also know what has been said in phone conversations or by email. Phone calls cannot be retrieved retrospectively, so a recording device has to be present at the time of recording. Taking the principle of subsidiarity into account, respondents state that they try to avoid this type of information gathering as it is considered to be intrusive, even though privacy legislation does allow it.[26] When it comes to email, older information could be retrieved. Email-boxes may be 'imaged' and stored in a database to search. This also goes for 'the digital environment' more generally. 'In the larger investigations, data recovery is a standard ingredient. This may become pretty complex because you have to take privacy regulations into account and when the data crosses the national border, this may be a problem' [Respondent 28]. Data carriers such as PC's, laptops, USB sticks and tablets can also be investigated with regard to content or activity (e.g. internet logs), as long as they are company property.[27] The growing use of BYODs (bring your own device, usually a laptop) may in this light prove problematic for investigators, as the investigation of these devices is not permitted. As mentioned before, private investigators lack the powers of investigation law enforcement has, and therefore their access is limited (though still quite extensive). Within the boundaries of available information, corporate investigators may, however, investigate more effectively than law enforcement would.

> Of course they [law enforcement agencies] may demand information and we will have to provide that. But often they don't quite know what kind of information they need. For example they ask for the laptop of the involved person. But with that they don't have access to our system, just the computer. You need authorised log in codes to access the system and they don't have that. I sometimes try to explain this but unless you're talking to someone from a specialised high tech team, they don't know what you're talking about. They don't understand how our systems work. Neither do I for some part but we have people here who do. Generally they just look at the laptop and stop there. There's an entire world of

25. NVB, above n. 15.

26. *Ibid.*

27. As long as they are accessible by the investigator. For example, when a work laptop is used and stored at home, investigators may only access it when the employee has handed it back to the employer. NVB, above n. 15.

information behind that which they'll never see. [Respondent 43]

4.2.2 Other Internal Systems

In addition to the aforementioned communication systems, there are many other internal systems that may provide information. Many companies, for example, use a key card system for employees to gain access to a building. These can be used to find out whether someone has been present at a certain site.[28] Track-and-trace or GPS systems are also used by some employers to keep track of their deliveries or vehicles, and these may provide information on someone's whereabouts. In addition, regular personnel files, such as a record of someone's work history at that employer, can be used as background information. A more controversial internal system is the blacklist. Although a blacklist meant for internal use is allowed by privacy law, it is obligatory to report sector-wide use of this beforehand to the data protection authority.[29] Many respondents indicate that they are not sure whether their blacklist meets the criteria, but they do keep a database with information on people who have been investigated or fired in the past.[30] These are often used as reference points in investigations (and in the process of hiring new staff). When an organisation has an in-house security department, this department often is the keeper of the blacklist. If not, another department (such as human resources) manages the list. In the latter case, investigators are not involved in the management of the blacklist (as they are not part of the organisation keeping the list). External investigative firms also keep their own records though, consisting of the documentation of their investigations. These are used as information for other investigations or background checks as well.[31]

Finally, the use of (hidden) cameras is not entirely free from controversy. Cameras may provide valuable information, for example when the footage can be used to ascertain which employee took money from the cash register. Although it is allowed to record employee's movements, privacy law prohibits the use of cameras in certain places (such as the bathroom). Furthermore, employees should be made aware of the possibility of camera surveillance.[32] 'We have many cameras placed in our buildings and people know this, they are made aware of it. When we have a missing item at a certain location, we can inspect the camera footage and look for suspicious actions that are not part of the work process' [Respondent 15]. Under certain circumstances, the use of covert cameras is allowed.[33] Respondents indicate that the use of covert cameras is the exception rather than the rule.

4.3 Open Sources

Much information can be derived from open sources. A large proportion of both professional and social life occurs online and for a person who knows where to look, the internet contains a lot of interesting information. In one of the observations, the investigations were organised in such a way that some investigators focused on doing 'desk research'. This contains the investigations of internal systems as discussed above, but also the investigation of open sources. One investigator was highly skilled in this type of desk research and had several (fictitious) accounts on social media sites so he had easy access to this information. Social network sites such as Facebook and LinkedIn may provide a broad overview of someone's life (e.g. posts, photographs, likes, sites followed) and professional network (which may be useful, for example, to show that a third party that is involved knows the involved employee).

In addition, there are some very valuable generally available or for-subscription databases. These might contain information on Chamber of Commerce records, name and address data and domain name registration. Many investigators have a subscription to these databases. Additionally, traditional media and the internet more generally (and search engines more specifically) could also provide a lot of valuable information to investigators.

4.4 Other Sources

Depending on the type of incident and the circumstances surrounding it, there are multiple additional methods of investigation. For example, observation can be useful, although most of my respondents did very few observations. Observing someone is allowed under privacy law, although not in every circumstance. In general terms, an observation is less likely to be considered a breach of privacy when it is done in a public place and for a short period of time. More intrusive forms of observation (such as dynamic observation using a tracking device) may be allowed, depending on the circumstances.[34] Observations (and the use of camera footage) are for example, used when an employee is suspected of sick leave fraud. Site visits may also prove useful to see whether the 'reality on paper' matches the 'actual reality'. 'For example, go and take stock for yourself and make sure that what's in the administration, is in fact what's in stock. To determine that, ok there is a possibility that the warehouse keeper or someone else took something' [Respondent 13]. Some organisations furthermore do a standard search of employees and their belongings when they leave the workplace.

> We also search people before they leave. We use a metal detector for that as well. Sometimes this may bring things to light. You know, situations where people take something that isn't theirs and that the

28. Although this circumstance alone is not sufficient proof, as people tend to use each other's key cards even when this is prohibited by the company code.
29. *See* Art. 22 under 2 sub b WBP; CBP, *Een zwarte lijst gebruiken* (2015).
30. This does not necessarily mean that the blacklist does not comply. Many larger companies have a privacy officer who is better informed on these issues than the respondents mentioned here.
31. NVB, above n. 15.
32. CBP, *Cameratoezicht op de werkplek* (2015).
33. NVB, above n. 15.
34. *Ibid*.

> alarm will ring. They're asked to empty their pockets and well, if something's in there that doesn't belong to you, you're going to have a good conversation with me. [Respondent 15]

Other activities of corporate security investigators include the evaluation (and correction) of previous investigations, the evaluation of internal control systems, the calculation of damages in light of a civil claim and the tracing of assets. When a report is made to the police (which often happens only after the internal investigations have been concluded), law enforcement information may also be used to investigate further. However, law enforcement agencies are very careful with information sharing, as some investigators from the observations noted:

> That's the thing. They *think* there's no room but there is. The shutters close on mention of information sharing but that's not necessary. When I report a crime to the police, I would like to get some information on their interrogations etc. They say, 'no that's impossible because of privacy'. They're so afraid to get it wrong that the solution is not to share anything. We don't need operational details, it would be very helpful if they could just give us directive information without them having to have to start an entire investigation. Just to let us know whether we're on the right track. [Conversation in observation 2]

5 The Interview: Confronting the Involved Person

The interview is the most important source of information for corporate investigators, according to respondents. It usually is the last phase of the investigations, in which all information that has been collected is used to confront the involved person. Interviews with witnesses often occur at an earlier stage as they are informative (adding to the big picture). Many corporate investigators have a law enforcement background and are experienced interviewers. However, there are notable differences between an interview and a police interrogation. For example, there is no formal caution at the start of the interview because the interviewee is not a suspect in the sense of a criminal procedure. However, respondents indicate that they do point out at the start of the interview that the interviewee is not obliged to cooperate and that he cooperates on a voluntary basis.[35]

> His statement is made freely, I mean if during our conversation he decides not to want to talk about it, ok that's his story. I'm not sure he's going to be better off with that but when someone walks out the door, he walks. I'm not going to grab him by the neck and say, ok now you're going to talk. [Respondent 15]

35. *Ibid*.

The voluntary nature of the cooperation of an employee should not be overstated. There is a definite power imbalance between the employee and the investigators (providing a service to the employer). Investigators stress their independence within the assignment they receive. 'We have our own set of rules on how we conduct our investigations and we give this to our client at the intake of the assignment. Sometimes they say, can't you do this and that. No, sorry. These are the rules, this is how we do things' [Respondent 2]. However, this does not mitigate the power imbalance much. An employee is technically free to refuse to cooperate – in practice, he or she can feel forced to cooperate with the investigations by his employer. Investigators are aware of this 'limited voluntariness'.

> We caution people at the start of an interview, so to speak, by saying they are not obliged to cooperate. But they feel obliged of course. Sometimes someone asks, what will happen if I don't? Well then I will have to talk to your manager about that. An interview is very confrontational. I dare say we give high priority to fair play, we stick to our own procedures. But we're not treating someone with kid gloves. If someone has done something wrong, it's ok to let him feel that. We are about finding the truth, which can be in someone's advantage too. If you did nothing wrong and we're totally off track, here's your chance to fix that. [Respondent 44]

The Privacy code of conduct, binding to private investigation firms and used by many other investigators as well, pays attention to the question of undue pressure:

> The mere questioning of someone by a private investigator produces a certain amount of pressure. As interviews are done on a voluntary basis, as a rule there will be no undue duress. It is hard to draw the line between what is and what is not allowed. Keen interrogation is in itself legitimate. It is thus allowed to confront someone denying involvement with evidence and to point out his weak position. Undue pressure is exerted, however, when physical pressure is used. Making false promises and verbal abuse are also illegitimate.[36]

In addition to the legally defined rules, most corporate investigators have their own guidelines for investigations and interviews. These include the right of representation by a lawyer or union representative and the general obligation for the investigators to treat the interviewee with respect and refrain from applying undue pressure and presenting false information.[37] Moreover, interviewees are given the opportunity to have a break and are offered something to drink and eat. 'As of late we also include this in the interview report – that someone has been treated correctly, had something to drink

36. *Ibid*.
37. *See* for example GrantThornton, *Grant Thornton Forensic & Investigation Services B.V. Reglement onderzoekswerkzaamheden* (2010).

and had to opportunity to use the bathroom. That's also to have proof of this for a possible court case of course' [Respondent 45]. Because 'the first thing a lawyer tries to do, also in a police investigation, is to discredit the statement that has been made by the involved person' [Respondent 44].

Some respondents empathise with the interviewee, saying that they can understand the position he or she is in during an interview. However, most state, for example, that

> you need to be completely neutral in these things. You didn't contribute to this misery, you're just hired to get a clear picture of the mess and fix it. You need to be professional about that. Of course, you need to be friendly. When someone needs a break, you offer him one and you record this in the interview report. 'At that and that time interviewee was very emotional and we took a break'. So you also report what time you continued, you give the man some water, maybe suggest that he takes a walk in the garden. And sometimes, I join them, have a smoke, then some other kind of conversation unfolds. And when he's ready, you reopen the interview. [Respondent 1]

Interviews are generally done by two interviewers. There are multiple reasons for this, one of the most important being the need to have a witness for what has been said during the interview. Furthermore, having two people present is beneficial to the expedition of the interview.

> One of us takes care of the conversation, the other takes notes. So, we can make a report of the conversation on the spot and print it out and then the interviewee can read it and sign. When there are corrections that need to be made we will adapt the document, print again and sign it. The interviewee signs for having been made aware of the content of the interview report and he gets his own print to take with him. It happens that people don't want to sign because they do not agree or because they want to talk with a lawyer. In that case, we sign it anyway. And sometimes people don't even want to talk to us. [Respondent 44]

As the cooperation is voluntary, people may refuse their assistance in an investigation. This could mean that he or she does not want to talk to the investigators, or that the interview takes place but the person will not answer relevant questions. As the above quote shows, the interviewee is asked to sign the interview report with the interviewers, which he may refuse to do. In this case, a note is made at the end of the interview report and in the final report (see also below).

5.1 The Interview Process

Respondents explain that although an interview is often done in a comparable manner, there are no specific standard ways to conduct an interview. Different interviewers have different styles. There is also a difference with regard to the type of person who is interviewed (a witness or an involved person). Interviews with witnesses are more informative than confrontational and often happen at an earlier stage. (Self-imposed or formal legal) rules regarding the interview with a witness are less stringent than when it comes to an interview with an involved person. It is required by privacy law that an involved person is made aware of the investigations he is subject to at the very beginning of investigations.[38] However, there are some exceptions to this rule, for example for the protection of the rights of others (including the client).[39] In practice, this means that involved persons are often notified about the investigations at the moment of their interview, which often is at the conclusion of the investigations. Although there are situations 'in which you need to talk to the involved person as soon as possible, you often postpone this interview until you know exactly which questions to ask, based on the information you gathered' [Respondent 2]. The situation is then also avoided in which the involved person might destroy incriminating evidence.

> In principle, you provide the involved person with the code of conduct for investigations at the earliest occasion, unless investigative interests are opposed to this. So in case you have to start your investigations and the involved person is still working there, there's a chance evidence will be lost. For example because he erases all files from his computer or removes and destroys physical documents from the administration. That would be a reason not to inform him just yet. You will first have to secure the evidence and only after that, when you know everything is safe, you will notify him. [Respondent 2]

Interviews may take a very different turn from what investigators had anticipated. It is therefore important to stay flexible when conducting an interview.

> Sometimes you decide on a certain tactic for an interview but it turns out very differently. I remember a case where we were expecting this person to be uncooperative and so we decided to start with a confrontation right off the bat. But we entered and he was very open and he wanted to talk to us. You start with a certain tactic but just like that it's useless and then you need to converse with someone in a different manner than you'd expected. And it also depends on the subject matter. Or for example when someone is very emotional. Of course there are parts you can prepare beforehand but when you discover during the conversation that the important stuff is somewhere else you have to let go of your prepared list and move to that subject. So you can devise a certain grid but in practice it seems that you need to be very flexible with that. [Respondent 5]

38. Arts. 33 and 34 WBP.
39. Art. 43 WBP.

As this quote shows, however, interviewers do apply certain tactics during an interview, and they prepare for it.[40] The level and depth of preparation depend in part on the information that is already available. When the interview is used as a close to the investigations, usually there already is much information and 'you can write much down in advance, you can make a draft of the interview report and confront him with it. Then you add his reaction, his declaration' [Respondent 44].
The two interviews that I was able to attend during the observations had a certain structure. This structure is also put forward by respondents.

> There's always a difference between interviewers, I always say, you need to do your own thing. But the standard elements are that you start with a social talk, an explanation of the context of the interview, his rights and sometimes his duties. So basically what's in our code of investigations. And usually, you move from a general conversation to more specific elements. In this conversation you need to explain your assignment also. So you use a funnel so to speak, as an interview technique. The more specific questions are somewhere in the middle of the conversation. And then you start to show your evidence to the interviewee. There's a turning point in an interview from informative to confrontational. That structure is always there. [Respondent 1]

In general, the interviewers seem to build the interview around three phases. The first of these is centred on pleasantries – the interviewers start with light conversation to make the person feel at ease. This includes small talk, for example about a person's job. The voluntary nature of the conversation is stressed in this phase. 'I want to tell you that you are here voluntarily, which means that you don't have to cooperate and when you want to leave, you are free to do so. But of course we hope you will cooperate with us' [Observation 2].
After the interviewee has had the opportunity to talk freely about what he thinks is the reason he is there, the interviewers start with the second phase, 'confrontation'. Here the evidence that has been gathered through other channels is used to confront the interviewee with 'the holes in his story'. The ambience changes from being amicable to more stern. Respondents state they treat the interviewee with respect and do not apply undue pressure. This was also the case during the interviews witnessed by me during the observations. The mere setting of the interview, however, could put pressure on the person, even when no boundaries are being crossed. Especially when the employee is without representation, he might feel pressure to talk even though he does not want to. The interviewers are experienced, and, as mentioned earlier, respondents indicate that interviews are done in couples, which brings a certain force with it.
The final phase of the interview is the conclusion. At this stage the important information that has been discussed is summarised and either typed up directly or the interview notes are checked to make sure they are complete. Most respondents prefer to finish the interview report on the spot.

> When it comes to an involved person, [drafting the report at a later time] may not be the best course of action because then you run the risk he will rethink what he has said. 'I said that but maybe it wasn't wise to do so, so I want it deleted'. When you correct the report directly, print it, let him read it and comment and ask him to sign, this risk is much smaller. [Respondent 2]

The atmosphere seems to change back to amicable in this last stage. The interviewers and interviewee might discuss what will happen next and what the motivation was for the transgression. If the report is typed up on the spot, the interviewee – in accordance with the adversarial principle – gets the opportunity to read it and comment on factual errors. He is then asked to sign the document, along with the interviewers. This is also voluntary – the interviewee is not obliged to sign. 'For example, this involved person X refused to sign his interview reports. We did sign, these were the statements he made to two witnesses [interviewers]. So if it comes to a trial, we can testify under oath about this' [Respondent 1]. If the report is typed up at a later time, the interview report is sent to the interviewee to comment upon and sign. Respondents do not deem it problematic if the interviewee refuses to sign the document. When this occurs, a note is made that the document has been offered to the person to read and sign but that he or she has refused to do so. Generally, this is considered to provide enough information to make the interview report usable.[41]
Interview reports differ in size, but they are often a summary of what has been said instead of a verbatim account. The interview reports available to me during my research were mostly limited to a few pages. This is not a good indicator of the duration of the actual interview – only the relevant parts of the conversation are summarised in the interview report. This means that the interviewers have quite some freedom in drawing up the interview report. However, the interviewee has the opportunity to amend the report when he thinks important parts are missing. The interviewee sometimes wants to exclude certain information from the interview

40. There are many (mostly US) textbooks, e-learnings and other professional information available on different approaches and interview techniques. In this paragraph the broader outlines of the interview as a source of information are described – these very detailed instructions on how to interview are beyond the scope of this article. Additionally, the fieldwork reveals that many corporate investigators feel that interviewing can be taught but much importance is given to experience and following one's own instincts. Although they state that there are no standard ways to interview, stressing the importance of flexibility, they seem to broadly follow the process as delineated in this paragraph. *See also* N.F. Coburn, 'Corporate Investigations', 13 *Journal of Financial Crime* 2006 (348).

41. Van Wijk *et al.*, above n. 21.

report, 'for example private information that his manager has no business knowing' [Respondent 45]. It happens that investigators honour the request of the interviewee, but only when the excluded information is not relevant for the case.

> And when someone wants to change something we don't agree with, we make a note of that and sign that too. Openness, transparency, completeness. Pro and contra. Those are important principles. It rarely happens that an interview report is reproduced in full in the final investigations report but such a comment will be mentioned in the report when relevant – either to support or to defy your conclusions. [Respondent 1].

The fieldwork reveals that using the methods of investigation discussed, corporate investigators are often able to provide a pretty complete reconstruction of the incident. Using phone records, combined with open sources such as social media, investigators can map who has been in contact with whom, where a third party lives, works, etc. Furthermore, investigations into financial records and other relevant documents can provide insight into fraudulent financial transactions. When it comes to theft from a shop, for example, cameras and employee log files can be very useful. Although all methods and sources of information described here are valuable, respondents tend to place most importance on the interview as a source of detailed information. Usually, the investigations lead up to the interview with the involved person(s). In these interviews, information can be checked, details added and errors corrected – that is, when the interviewee decides to cooperate. All this information needs to be made available to the client in a concise and clear way. To achieve this, an investigative report is written.

6 Reporting on the Investigations

Once the investigations have been concluded and the questions that were the basis for the assignment can be answered, the information has to be made available to the client. Reports are often quite short and to the point, as respondents indicate that this format is best appreciated by their clients. A report needs to be clear on the facts and easy to read.[42] Depending on the nature of the assignment and the complexity of the incident, reports may be merely 2 pages (not including appendices), while others may span 150 pages. 'The size of a report varies between assignments but thirty pages is usually about the length for us. Sometimes they are very factual, then a lot of appendices might be attached, for example interview reports' [Respondent 36]. Some investigators prefer to use appendices, while others prefer to integrate relevant parts of interview reports or other findings in the report without them being attached. 'These interview reports are for internal use, to build our case. They are not an integral part of the eventual report. We do use them to quote from, especially crucial parts' [Respondent 5].

It is difficult to give a standard format of an investigative report, as there are notable differences in the way the findings are presented. However, most investigative reports contain the following subjects:[43] 'A report is typically formatted like, what was the assignment, what was the scope, what did we do and what did we find?' [Respondent 36]. Some investigators also add some legal information, a preface with some kind of disclaimer or other relevant information. Opinions seem to differ with regard to the necessary information for a report, although there is some consensus that a report should be transparent about the presented findings and how these have come to the fore. The client needs to be able to assess the validity of the report and interpret its findings.[44] Some commentators suggest that it is necessary to have a predetermined goal for the investigations, for example a report to the police or a dismissal.[45] When agreed upon between client and investigator, this predetermined goal is usually presented in the report. However, in practice the decision about what to do with the results is often made only after the results are clear. 'For example, we hand in the report and the client says, "I didn't know it was this serious, I want to report to the police after all". Ok, so then we go and report to the police' [Respondent 1].

The standard of evidence in a civil procedure is lower than that which is used in criminal court. 'Improperly obtained evidence is not as problematic for the procedure in civil court. A civil judge will not readily dismiss evidence, he might reprimand you for it but he has heard it anyway and will use it. Plus, often it is not the only evidence you have, you can build your case with the other evidence as well' [Respondent 50]. Cases may also be concluded entirely without the involvement of a judge,[46] which makes the way evidence is gathered even less of an issue in that sense. However, respondents indicate that they feel it is important to 'go by the book', both in a moral sense and because in many cases the decision about how to handle the matter is made only after the investigations have been concluded and the report is handed in to the client. Some respondents therefore state that they try to aim for the standard of evidence that is used for criminal investigations. 'You

42. L. van Almelo and P. Schimmel, *Feiten maken het recht; Forensic accounting revisited* (2014).

43. There are some (very general) standards provided for forensic accountants, but not all corporate investigators use them. NIVRA/NOvAA, above n. 14.

44. J.F. Rense, 'De private onderzoeker; (ver)plicht tot hoor en wederhoor?', 78 *Maandblad voor Accountancy en Bedrijfseconomie* 76 (2004).

45. P. Schimmel, *Fraudebeheersing; een leidraad van preventie tot detectie* (2011).

46. C. Meerts, 'Over pragmatisme en strategie verschillende routes voor private opsporing en afhandeling van onregelmatigheden binnen organisaties', 56 *Tijdschrift voor Criminologie* 115 (2014).

have the highest standards for the burden of proof there, beyond reasonable doubt. If it complies with that, it will comply with the others as well. So this way, these other settlement possibilities will all remain an option' [Respondent 1].

Before the report is handed over to the client, the involved person will usually get the opportunity to read the relevant parts of the report and comment on it. This implementation of the adversarial principle is derived from accountancy rules; however, most respondents state they comply with this rule even if they do not have an accountancy background.[47]

> And especially when it concerns an involved person – you're required to do so because it's a person-orientated investigation – we use the adversarial principle. The first phase of that is to invite him to answer some questions. And the second is that when you make a final draft of your report containing parts that concern that person, you give him the opportunity to react to it. So he can read it and comment on it. And those comments are added to the final report…. And I think this is a good thing and very reasonable. I think that's very important, it can't be the case that you just go about your investigations without ever speaking with this person and still write a report about him. Obviously, that's not right. [Respondent 5]

Not every involved person takes the opportunity of reading the relevant parts of the report. Respondents indicate that this is not necessarily problematic, however it does mean that caution should be applied when presenting findings.

When the adversarial principle has been applied and the draft is amended, the report can be finalised and signed. Not every investigation yields enough information to answer the questions asked in the assignment. When this is the case, a report is made about the findings and the lack of certainty is stated. Whether or not a conclusion of findings is drawn in this final report depends on the type of investigator. For example, forensic accountants consider drawing conclusions from the presented facts or providing advice to their client in a report 'not done'.

> We are hired for the *fact finding*, a forensic accountant does not assign value or interpret findings. At the most, the report will state the rules that are applicable and the behaviour that it concerns. The rule and the behaviour will be presented side by side but it will not be stated that the conduct was improper. Clients always ask for a conclusion, 'just write down what you think'. But that would be subjective. The report sticks to the facts. [Respondent 36]

Others prefer to give some advice on how to proceed but the extent of this advice also differs among respondents. This respondent, for example, does include some advice on the possible ways of settlement but provides no opinion on the best solution in the current case:

> Every case is different, the interests involved are different. Every time you're faced with a different web, different tensions. The outcome is different every time. But you know, I don't really care about that. We have a job to do and do it well. You can provide your client with the options but I'm not going to be the one to say, this is the way to go. Who am I to say they should report to the police? [Respondent 1]

Corporate investigators with a legal background are more inclined to provide advice on how to proceed:

> And eventually you will come to the point that you write your report and explain your findings but also draw conclusions based on that. That could be that there must be measures taken against certain persons or that the structure of the organisation should be changed…. And it could also lead to the question whether or not the incident should be reported to the police. And that's often a tough one to answer. [Respondent 30]

The extent to which corporate investigators may influence decisions about settlement of the incident differs; however, respondents indicate that the actual decision is not taken by investigators. The client is the one who decides. In in-house security departments, the division between the investigators and the decision makers may get blurry at times. 'Whether or not it needs to be reported to the police is a decision that does not concern HR. They want to take the decision, but it will be me who sees whether or not I find it useful. The policy is, report every time, in practice it hardly ever happens. I'm the one who has to go there and file the report so I'm the one deciding' [Respondent 48].

> We do the investigations and that's it. Two of my colleagues have a different opinion, when they say someone's guilty he should be fired, another has a more nuanced take on the matter. Our job is the investigation, getting the evidence and building a case that would hold up in court if necessary. The decisions lie with the involved manager and HR. [Conversation in observation 2]

Interestingly, respondents working in an in-house corporate security department indicate that not every investigation merits a report.

> We don't always write a report, we get a lot of rubbish cases. In that case, it's no use to write an entire report. The rule is that when they want to fire someone, we do write a report for the involved business unit, with an advice attached, for example about the processes that made the transgression possible. But when they are just going to give the involved person an official warning, there will be no report. Maybe

47. Rense, above n. 44.

> we'll give some advice but nothing written down. When there is no report, your notes, the journal and our registration system 'are the report'. [Respondent 43]

In such a case, the case notes are simultaneously the final product of the investigations.

7 Discussion: Differentiation?

This article has explored the investigative methods that are used by corporate security in its investigations into incidents within organisations. Having to work without the investigative powers of law enforcement agencies might pose some problems for corporate investigators, but it also provides possibilities. There are instances when the information provided by the client and gathered through the cooperation of various people proves to be inadequate to reconstruct what happened. Corporate security cannot force people to cooperate[48] (although a certain amount of duress might be present), nor is it allowed to, for example, enter and search private premises. This may mean that a report to the police will be necessary if clients want to investigate the incident fully (which they may not).

Conversely, corporate security is more flexible than the police are.[49] It is responsive to clients' needs, and because of the close connection to the client and a contractually created duty of confidentiality, much information is readily available. Furthermore, because of this and the absence of the need to wait for formal approval from for example a judge, corporate investigations can be executed and concluded fairly swiftly. The absence of formal investigative powers may have sparked the creativity of investigators to take a broader approach to investigations and use methods of investigation that may be regarded as more private in nature. The use of forensic accounting techniques, IT tools and open sources (for a large part digital social networks) does not fall in the category of 'traditional police work' (although the police are also increasingly making use of these techniques and information sources).

This article has focused solely on the methods of investigation that *private* investigators have at their disposal. As such, the methods of investigation that law enforcement officials might use have not been discussed, and a full-blown comparison between public and private is not within the scope of this article. One important defining characteristic of law enforcement, though, is its power of investigation and the legitimate use of force. Respondents who have previously worked in public law enforcement indicate that they feel handicapped by not being able to use formal powers of investigation. The lack of investigative powers and the use of more specifically private investigation methods mark a line of differentiation between public and private actors in this field (external differentiation). This seems to be underlined by the avoidance of 'criminal justice terminology' by corporate investigators.

In addition to the private investigation methods that may be used by corporate investigators, another defining characteristic of the field is the diversity of people working in it. Although there are many former police officers working in corporate security, there are also numerous 'private actors' active in the sector: forensic accountants,[50] private detectives[51] and in-house security departments (consisting also of people with a background specific to the sector of the company where they work).[52] In more recent years, lawyers have also established a place in the private investigation industry.[53] These different actors also bring their own expertise and skills to the table. The internal differentiation within this field may also be discerned in the different rules and regulations that apply to the different actors. And yet, although there certainly are differences between these actors, there is also a large common ground between them. Together, these actors – from varying backgrounds, with specific occupational cultures, all lacking formal investigative powers and yet all enjoying a high degree of discretion and operational flexibility – constitute the corporate security field in the Netherlands.

Thus, we might conclude that the field in which corporate security moves is characterised by differentiation. First, externally, there is differentiation between private actors and public authorities in relation to the methods used, the power to use them and the rules one has to comply with. Second, there is internal differentiation within corporate security, according to professional backgrounds. This article has focused upon the first of these – the public/private differentiation – by taking a closer look at corporate investigation methods. As Williams has previously noted, public and private actors are not interchangeable here.[54] Interestingly, corporate security respondents seem to (symbolically) emphasise this differentiation between them and law enforcement, by avoiding the use of 'law enforcement terminology'. Private corporate investigators have created a formalised professional private sphere, in which they use their skills and expertise to provide clients with the services they need. Previous research has remarked upon the benefits for organisations of such a private solution over a police investigation (and subsequently, a criminal tri-

48. Neither can the police, of course, although they do have the power to summon documents, enter buildings without consent (when this is approved by a prosecutor or judge), etc.
49. Williams (2005), above n. 3.
50. *Ibid.*; J.W. Williams, 'Private Legal Orders: Professional Markets and the Commodification of Financial Governance', 15 *Social & Legal Studies* 209 (2006); Williams (2014), above n. 7; Van Wijk *et al.*, above n. 21.
51. Gill and Hart (1997), above n. 3; M. Gill and J. Hart, 'Private Security: Enforcing Corporate Security Policy Using Private Investigators', 7 *European Journal on Criminal Policy and Research* 245 (1999).
52. Nalla and Morash, above n. 3.
53. B.C.G. Jennen and H.J.TH. Biemond, 'Het interne fraudeonderzoek: enkele juridische overwegingen', 4 *Tijdschrift voor de Ondernemingsrechtpraktijk* 57 (2009).
54. Williams (2005), above n. 3.

al).[55] Thus, differentiation rather than convergence between public and private seems to be the key concept in the field of corporate security.

One implication of this differentiation between public and private and within the private sphere is the difficulty with regard to oversight over the activities of corporate security. As mentioned, different actors have different regulations to comply with, some more formal and binding than others. The distance between public and private and the large proportion of activities that stay completely in the private sphere make it all the more difficult to control the applications of these rules. Although not as intrusive as the formal powers of investigation of law enforcement, corporate investigations may have a large impact on the lives of the people involved: a lot of information may be gathered about a person, and the consequences (loss of employment, repayment of damages, a criminal prosecution) may be considerable. This research has not found indications of illegal action by investigators – however the looseness and diversity of rules and the lack of oversight make for some potential for abuse.[56] Even when all the (formal or self-imposed) rules are followed, the impact of private corporate investigations may be substantial, and there is also the possibility of the abuse of the power imbalance that exists between the organisation and the person(s) under investigation. More research into the field of corporate investigations and private settlements is therefore warranted. One interesting line of research would be to focus on the interaction between the rules on the one hand and the behaviour of investigators in practice on the other.

55. *Ibid*.; C. Meerts, 'Corporate Security: Governing through Private and Public Law', in K. Walby and R. Lippert (eds.), *Corporate Security in the 21st Century: Theory and Practice in International Perspective* (2014) 97.
56. There are some disciplinary and civil cases about the behaviour of investigators. *See*, for example, ECLI:NL:TACKN:2016:49, ECLI:NL:CBB:2016:148 and ECLI:NL:RBMNE:2015:5572. (Grave) misbehaviour of investigators is not very readily assumed.