

ORIGINAL ARTICLE

## How the detection of insurance fraud succeeds and fails

NICOLA J. MORLEY, LINDEN J. BALL, & THOMAS C. ORMEROD

*Lancaster University, UK*

### Abstract

Insurance fraud is a serious and growing problem, and there is widespread recognition that traditional approaches to tackling fraud are inadequate. Studies of insurance fraud have typically focused upon identifying characteristics of fraudulent claims and claimants, and this focus is apparent in the current wave of forensic and data-mining technologies for fraud detection. An alternative approach is to understand and then optimize existing practices in the detection of fraud. We report an ethnographic study that explored the nature of motor insurance fraud-detection practices in two leading insurance companies. The results of the study suggest that an occupational focus on the practices of fraud detection can complement and enhance forensic and data-mining approaches to the detection of potentially fraudulent claims.

**Keywords:** *Fraud detection, insurance fraud, ethnography*

### Introduction

The Association of British Insurers (ABI) suggests that fraudulent claims cost the UK insurance industry over £1 billion a year, representing a 30% increase over a two-year period to 2001 (Association of British Insurers, 2001). The complexity of the problem matches its magnitude, and this complexity arises from a number of sources. Fraud is dynamic: when the industry uncovers one ‘scam’ (i.e. specific type of fraudulent activity) and puts up barriers to prevent its reoccurrence, another scam takes its place. Motivations to commit fraud vary, from opportunistic individuals submitting a fraudulent claim as a way of recovering their premium, perhaps encouraged by a shift in public attitudes towards the perception of insurance fraud as a victimless crime, through to criminal networks that use fraud as a regular source of revenue generation. Moreover, the legal, organizational and commercial constraints under which the insurance industry operates often impact negatively upon the success of existing fraud prevention, detection and investigation practices. In this context, the insurance industry is actively seeking solutions, typically technological, that might address the increasing problem of fraud.

In this paper, we present an observational study of claims-handling practices in two major UK and multinational insurance companies. The study formed part of a larger project to specify and develop technologies for tackling insurance fraud (Ormerod, Morley, Ball,

---

Correspondence: Dr L. J. Ball, Department of Psychology, Fylde College, Lancaster University, Lancaster, LA1 4YF, UK. E-mail: l.ball@lancaster.ac.uk

Langley, & Spencer, 2003). Empirical studies of insurance fraud have typically focused upon identifying characteristics of fraudulent claims and claimants. This focus is apparent in the current wave of interest in the industry in applying approaches such as cognitive interviewing (for a description see Kebbell, Mile, & Wagstaff, 1998) and voice stress analysis (e.g. Hovarth, 1982) that have been employed in other domains of forensic investigation, as well as data-mining techniques developed specifically for fraud detection ("Hunter Production Information", n.d.). Little empirical research, however, has examined the roles that employees of insurance companies play in fraud detection and investigation, or factors that might limit the effectiveness of fraud prevention practices. The present research aimed to address this omission by adopting an ethnographic approach to observation (e.g. Ball & Ormerod, 2000a, 2000b) in order to understand the cognitive, social and organizational contexts in which claims handling occurs.

Employing an ethnographic approach complements the statistical, interview and questionnaire methods used in studies of fraud types and fraudster profiling by providing a detailed, longitudinal and independent evaluation of issues and activities surrounding how the industry deals with fraud. Ethnographic studies enable the observation and discursive evaluation of best- and worst-practice examples that the proponents of such practices may be unaware of, or which they may be unable or unwilling to report or evaluate without bias. In our study, we identified a number of practices and skills that existing industry processes fail to support properly, and in some cases actively undervalue or ignore, but which we believe offer opportunities for positive change. We argue that technological developments for fighting fraud can only be effective if used in tandem with processes and techniques that capitalize upon skills and knowledge held by staff at all levels of experience within the industry.

In the remainder of the paper, we overview what is known about the nature of fraud and of fraudsters, and discuss the relative strengths of traditional and new approaches to tackling fraud that capitalize upon such knowledge. We then outline the ethnographic method, and describe its use in a study of the motor insurance departments of two insurance companies. The observations focus upon three levels of activity in fraud detection: contributions that individuals make, organizational issues, and technological factors. We conclude by evaluating the relative contributions to tackling fraud of a forensic approach, which focuses upon identifying and treating the characteristics of fraud types and fraudsters, and an occupational approach, which focuses upon identifying and supporting all levels of expertise among the industry staff charged with the task of handling claims.

#### *Understanding the nature of fraud and of fraudsters*

There are numerous ways that people commit fraud. Gill, Woolley, and Gill (1994) define fraud as "knowingly making a fictitious claim, inflating a claim or adding extra items to a claim, or being in any way dishonest with the intention of gaining more than legitimate entitlement". The Crime and Fraud Prevention Bureau annual report (2000) cites four main types of fraud in motor insurance and their associated levels of occurrence as: completely false claims (12%), deliberately misrepresenting the circumstances of the claim (32%), inflated loss value (39%), claiming from multiple insurers (3%), with 14% being attributable to other types of fraudulent claims. Yet there is disagreement within the industry as to the best working definition of insurance fraud (Doig, Jones, & Wait, 1999). Some companies consider exaggerating a claim to constitute fraud, whilst others are more concerned with classes of systematic fraudulent activity such as staged accidents, false documents and misrepresentation of information at the proposal stage. The problem of

defining what constitutes fraud makes the task of tackling it more difficult because it is not clear at what level to focus anti-fraud measures.

There are also several types of fraudster, classified by Clarke (1989) as “the opportunist”, “the amateur” and “the professional”. The opportunist takes advantage of a genuine loss to commit fraud, for example, by claiming alongside genuine losses for items not stolen in a burglary. The amateur may start by committing opportunistic fraud and then take a step further, for example, submitting a claim for items stolen in a burglary that never took place. The professional, arguably the most serious type of fraudster, engages in systematic frauds both individually and in organized networks. Whether organized networks are to be found in all insurance domains is unclear. However, there is considerable anecdotal evidence that they exist in motor insurance and the potential for the spread of organized networks to other domains clearly exists.

Research has also focused on trying to understand why people commit fraud. Personal circumstances and a resentment of insurance companies appear to be major determinants affecting a person’s willingness to commit fraud (Gill et al., 1994). Trying to distinguish a fraudster from a genuine claimant based upon personal and social characteristics alone is, however, problematic. Research categorizing a sample of fraudulent claims has suggested that fraudsters show characteristics that make them for the most part indistinguishable from the genuine claimant (Dodd, 1998). The fact that professional fraudsters typically do not use genuine identities compounds this difficulty.

A large number of legal, commercial and organizational factors interact with the different types of fraud and varying motivations of fraudsters. A legal agreement between insurer and insured is based on the notion of “utmost good faith”, meaning that each party is legally obliged to reveal to the other any information that might influence the contract between them, even if it is not explicitly asked for. This agreement relies on trust and honesty on behalf of both parties. The competitive nature of the insurance industry means that it is very easy for clients to obtain a policy. This places pressure on the processes necessary to validate information submitted to the insurance company in order to check that both sides uphold utmost good faith.

Customers judge companies on the perceived efficiency of their procedures, such that scrutiny of policy information or claims information might reflect badly on their customer service reputation. In addition, companies are often reluctant to admit the scale of fraud problems to their shareholders and policy-holders (Doig et al., 1999). Moreover, increasing consumer awareness (e.g. through consumer journalism programmes) means that one badly handled claim can undo millions of pounds worth of advertising (Clarke, 1989). Fraud is also difficult to prove legally, and may incur further costs when police and legal teams are involved, without any financial outcome for the company beyond the recovered claim. Consequently, insurance companies are often reluctant to prosecute offenders, and sometimes this means that fraudulent claims end up being paid. It also means that there is little in the way of a deterrent for potential fraudsters beyond a failed claim.

### *Approaches to detecting potential fraud and fraudsters*

Despite the problems inherent in dealing with fraud, fraudulent claims can be, and indeed are, detected. Anecdotal reports from discussions with fraud managers at the start of this project suggested that detection typically occurs through the discovery of anomalies or inconsistencies in the information surrounding the claim (e.g. when the circumstances of the claim do not match the account given by the claimant), identification of patterns of claiming behaviour (e.g. repeated claims for similar losses), or recognition of inappropriate

claimant characteristics (e.g. aggressive manner, uncertainty and hesitance in supplying information). Investigators, often based in special units in larger companies, receive suspicious claims and investigate them further in an attempt to repudiate fraudulent claims. The process of investigation generally involves seeking further information, either from the claimant or from third party sources, and building up a clear account of anomalies and inconsistencies in the claim coupled with potential motives of the claimant.

The responsibility for detecting fraudulent claims in insurance companies rests heavily with staff at the front line of the claims-handling process. Claims handlers are often inexperienced, with typical company lifetimes of less than one year, and they often lack sufficient or appropriate training in fraud detection (Doig et al., 1999). Anecdotal estimates (from discussions with fraud managers in the insurance industry) of the rate at which fraudulent claims are detected are as low as 10%, suggesting that large numbers of fraudulent cases remain undetected. Specialist units and expert investigators rely upon others spotting suspect claims in the first place, and must therefore be able to discriminate quickly between claims that carry a high level of fraud likelihood and false positives, that is, genuine claims that appeared suspicious to an inexperienced staff member.

In order to increase the chances of detecting fraudulent claims by inexperienced staff, companies have traditionally provided claims handlers with lists of fraud indicators against which to check incoming claims. Doig et al. (1999) report two insurance companies who acknowledged using this type of approach to tackling fraud. A fraud indicator is a heuristic, based on company experience, which describes a factor believed to be indicative of potential fraud. Each company we have worked with has their own set of indicators, though there is considerable overlap across company lists. Commercial confidentiality prevents publication of an exhaustive list of indicators. More importantly, companies do not want the public to have access to such information because the indicators would lose their predictive power if potential fraudsters became aware of them. However, we can illustrate the concept of fraud indicators with some widely known examples. Some indicators check verifiable data. For example, the date of vehicle registration can serve as an indicator of a staged theft: modern expensive vehicles typically have high quality locks that would be difficult to open by an opportunistic car thief. Other indicators are more subjective. For example, a claimant who adopts an inappropriately nervous or aggressive manner in talking to a claims handler may indicate a potential fraudster. A decision procedure may accompany fraud indicators whereby claims that trigger a number of fraud indicators higher than a given threshold become targets for further investigation.

The fraud managers we spoke to revealed that within the industry the problems with traditional fraud indicators are now widely recognized. As our examples illustrate, individual indicators are not predictive of fraud – thieves do steal thousands of newly registered vehicles from genuine claimants each year, and there are many reasons other than fraudulent behaviour as to why claimants might appear nervous or aggressive. Logically, individual indicators are predictive of fraud only if accompanied by related indicators. However, simply summing the number of triggered indicators means that the interactivity between indicators is lost. Consequently, these approaches tend to generate large volumes of false positives, which clog up the investigations units of companies while impacting negatively on customer relations. Moreover, lists of fraud indicators fail to reflect the dynamic nature of fraud. Arguably, the use of static fraud indicators makes it *less* easy to detect new fraud variants than having no lists of indicators at all, since anomalies associated with new fraud variants will not trigger old indicators.

Insurance companies have taken further proactive steps to improve fraud detection during the claims-handling process. For example, the industry has developed several databases to assist in the detection of anomalous information at the claims stage. Examples include the Claims and Underwriting Exchange (CUE) and the Motor Insurance Anti-Fraud and Theft Register (MIAFTR). The aims of these databases are threefold; First, they provide a way of verifying the information supplied by claimants. Second, they allow companies to assess whether claimants have a history of suspicious or similar claims. Third, they provide repositories for sharing information about claims histories across companies and with other parties. Some companies restrict the use of databases such as these to specialist investigators, while other companies have attempted to introduce their use into the front-line of claims handling.

Like indicator approaches, database systems present problems for the detection of fraud. In particular, the quality of data held within such databases can be variable. Fraud managers report that data entry is often done over the telephone, or based on information supplied by the client, and will often be done independently and repetitively for each transaction that the same customer has with a company. There are therefore many opportunities to introduce noise into record sets, such as misspellings, missing items, duplicate data, and outdated information. An additional concern for databases such as CUE is that they are very specific to names, and fraudsters can easily change these. Consequently, searching database systems can lead to problems, both with the failure to find expected records, and the generation of false positives through erroneous matches.

Attempts at understanding insurance fraud have focused primarily on understanding the characteristics of frauds (Clarke, 1989, 1990; Dodd, 1998; Doig et al., 1999), and relied heavily on potentially inadequate methodologies such as sampling of fraudulent claims, interviews and surveys. Litton (1990) argues that this research should be treated with scepticism because it is typically sparse and often anecdotal. Despite this cautionary note, recent technologies and processes have tried to address some of the problems inherent in inexperienced staff and noise in databases by using advanced intelligent software coupled with a detailed understanding of the nature of fraud and fraudsters. One approach is to capitalize upon existing databases while overcoming problems of noise in the data using data mining (see Dunham, 2003 for an introduction to the data-mining approach). Data-mining techniques can detect anomalies between client-supplied data and existing datasets while remaining sensitive to minor mismatches that are likely to generate false positives, and allow the detection of patterns of fraudulent activity (e.g. patterns of repeated claim activity) among complex data sets. The software program Hunter (“Hunter Product Information”, n.d.) is an example of this type of technique.

Other new technologies draw upon profiling approaches used in criminology and forensic investigations, borrowing techniques such as cognitive interviewing (Kebbell et al., 1998) and voice stress analysis (Hovarth, 1982). Recent media reports point to insurance companies beginning to publicly acknowledge that they are using this type of technology in their bid to tackle fraud (cf. Steed, 2003). These approaches identify clients who display characteristics associated with fraudsters. There are also approaches that combine profiling, data-search and fraud indicators (see “Fraudscope – What is it?”, Anon, n.d.).

These technological approaches show promise but are largely unproven. One concern is that the current wave of technological and process fixes seems to have been developed without a full understanding of their users, that is, the claims handling and investigation staff within the insurance industry. The systems focus upon detecting anomalies, the corollary being that claims-handling staff are not themselves good at spotting anomalies in

claims data. Yet, as we report in the study described below, this assumption is incorrect. It is now widely recognized in other domains of human interaction with computing technology that a detailed understanding of the needs, competencies, frailties and expertise of the target users of systems is an essential part of design (e.g. Schneiderman, 1998). Thus, we set out to extend our knowledge of insurance fraud beyond a forensic focus upon the fraudster, focusing instead upon the occupational characteristics of industry staff responsible for identifying fraud. We therefore undertook an in-depth programme of research to investigate current practices in fraud detection.

### *The study*

Our research adopted an ethnographic approach to empirical study, using techniques such as interviewing, participant observation, non-participant observation, and practical hands-on experience, to develop a description of the process of fraud detection as it occurs in the complex environment of insurance practice. The long-term, situated, and intensive nature of ethnography facilitates an understanding of what people actually do, rather than simply engendering a report of what people think they might do when questioned at interview (cf. Viller & Sommerville, 2000). Many researchers support the use of ethnography to inform systems design, and have demonstrated its benefits (e.g. Anderson, 1994; Ball & Ormerod, 2000a,b; Bentley et al., 1992; Forsythe, 1995; Hughes, King, Rodden, & Andersen, 1994; Hughes, O'Brien, Rodden, & Rouncefield, 1997; Hughes, Sommerville, & Bentley, 1993; Suchman, 1987).

Ethnography lends itself to establishing a comprehensive picture of work practices and insights into how best to support such behaviours by means of technology and changes to current processes. Unlike survey and interview techniques, which are geared primarily towards eliciting an individual's personal perspective on their work processes, ethnography renders visible the social complexities of work activities, enabling the investigation of the use of technology as a feature of this social process. For example, ethnographic techniques might afford an understanding of how, when and whether current anti-fraud measures are used by claims handlers and investigators, what behaviours are best supported by computational techniques, what activities are best left to human intervention, and how to implement technological support systems with minimal disruption to effective practices that are currently in place. Our research focused on two leading insurance companies. A detailed longitudinal ethnography was undertaken in Company A. To extend the generality of our research findings, a follow-up study was undertaken in Company B.

### **Method**

The main ethnography consisted of observation and interaction in two different departments of Company A, a major multinational insurance company. The first department had responsibility for claims pertaining to commercial vehicle policies. The second department mirrored these responsibilities for personal vehicle policies. The ethnography lasted for two months and took place during regular working hours. During this period, the ethnographer sat with claims handlers, attended meetings and training courses, and observed work practices, on occasion asking questions about work activity and encouraging staff to talk aloud whilst completing claims-handling tasks. Observations were interspersed with periods of field-note writing to ensure that each part of the day was sampled across the two-month period. Three types of data were collected: first, audio recordings of conversations, think-

aloud protocols and interviews; second, field notes made during the two months; and third, samples of documents collected to illustrate work practices.

The ethnographer also spent one week observing the work practices of Company B, another leading company that specializes in direct sales of insurance policies. The ethnographer spent much of this time in the personal motor insurance claims department. Because of the short duration of the study at Company B, it was not possible to sample departments across different times of the day or corroborate evidence information gained from conversations with staff. Subsequent discussions with staff confirmed, however, that the observations were typical of the company's work practices.

## **Results**

The ethnographic research identified three key elements that impact upon the ability of a company to detect fraud: (1) organizational influences on the claims and fraud processes; (2) the role played by the individual within the claims and fraud processes; and (3) technological concerns pertaining to both the organizational and individual levels of company-based activity.

### *The organization*

Company A had strong organizational goals that dictated the nature of their claims procedure, specifically how the company approached the problem of fraud. The ethnography identified three key issues concerning the organizational goals that impacted upon fraud detection. These issues concern responsibility and incentives for fraud detection, case ownership and feedback on outcomes, and communication and integration of fraud detection within regular claims-handling activities.

Company A placed a strong emphasis on achieving high customer service standards by ensuring speedy and efficient throughput of claims. This is exemplified by the way in which the claims department was organized. Everything was focused towards the attainment of these goals. For example, large screens above the telephone operatives indicated the number of available operators, how many calls were waiting and how many calls had been taken that day. Large white boards listed the team's performance and dictated their targets and goals for the coming week. Staff had to be logged onto the telephone system at all times and had to enter a code detailing the reason for logging off. To ensure speedy and efficient notification of a claim, the company employed several groups of claims handlers, based at various sites around the UK, whose main responsibility was to record information about new claims. These were referred to as the Notification of Loss teams (NOL). Another set of claims handlers, the claims management group (CM), had the responsibility of ensuring fast and efficient claims settlement.

The company focused considerable effort and resources on monitoring the quality and quantity of the work of the claims handlers in both NOL and CM groups. This was the responsibility of the senior claims handlers and team leaders. They would listen into conversations between clients and telephone-based claims handlers in NOL, monitoring the number of calls taken and the percentage of time logged onto the phone systems. Those managing the claims further down the line at CM would also be monitored for the number of claims they processed each day and the number of pieces of correspondence they successfully dealt with. A sample of all claims handlers' files would be checked to ensure they had followed correct procedures. Staff success on these quality assurance procedures dictated their likelihood of personal development within the company.

Tackling fraud was not observed to be a company-wide organizational objective but the company did have a fraud initiative in place. Two members of senior management staff were responsible for delivering the company's fraud initiative. In the year prior to our study, they had implemented a procedure for identifying fraudulent claims in NOL and CM groups. Delivery of the fraud initiative procedure to the claims departments was accompanied by a half-day training session for staff in each group. This procedure involved the construction of a set of fraud indicators developed in-house that reflected the company's knowledge about indicators of potentially suspect claims. For each new claim, the claims handlers in NOL completed a fraud indicator sheet. Designated claims handlers (hand picked by senior site managers and the fraud team) acted as referral points for any claim demonstrating a target number of fraud indicators. They referred suspect claims to a loss adjuster (usually a third-party company specializing in verifying claimant information and assessing the circumstances and costs of a claim) who carried out further investigations. A strength of the company's approach to tackling fraud was that it had a formal mechanism in place at the very front end of the claims process where fraud is most likely to be identifiable. The company reported financial savings arising from withdrawn and rejected claims since the inception of the new fraud initiative of the order of a 5 to 1 savings-to-cost ratio. In addition, the fraud initiative raised the general awareness of fraud among claims handlers, thereby increasing the potential for identifying suspicious claims.

Despite apparent gains, the implementation of the fraud initiative appeared to be hindered by the key company objective of fast claims throughput. Emphasis on speedy settlement was incongruent with the necessary delay incurred by a requirement to investigate a claim. Thus, few suspect claims were referred for further investigation. Staff assessment criteria, in general, provided no incentive for fraud detection; indeed, they appear to have acted as a disincentive. Achievement targets and quality assessment checks focused the claims handlers' efforts on the quantity of claims dealt with rather than on the specific features of an individual claim. Thus, claims handlers demonstrated a reluctance to refer claims that fraud indicators had identified as potentially suspect and would readily dismiss them by identifying additional factors (e.g. low vehicle value, low claim value, no previous claims with the company, length of insurance history with the company) which they felt negated the fraud indicators identified. The problem of achievement targets was compounded for staff designated as referral points for fraud cases, whose performance assessment was adversely affected by other claims handlers referring suspect claims for them to examine. These referral staff frequently complained that their role interfered with the key objective of claims throughput and that they struggled to meet their targets.

A second limitation on the likelihood of NOL staff detecting and following-up suspicious cases was the lack of ownership and feedback about cases; claims handlers did not deal with a claim from notification through to decision. Thus, they rarely received feedback upon the outcome of a claim. In addition to proper incentivization, ownership and feedback are vital for improving people's fraud-detection practices. Ownership influences claims handlers' knowledge of the detailed circumstances surrounding a claim, affecting their ability to detect inconsistencies and anomalies as further information is supplied. Feedback serves a key learning role, building up claims handlers' general knowledge about the natures of genuine and fraudulent claims. Moreover, feedback would allow staff to find out reasons why suspect claims are sometimes paid (for example, due to lack of evidence), which in turn should make them more efficient in making choices about which cases to refer.

Lack of ownership reflects the fast throughput of claims. New correspondence surrounding a claim was allocated in the NOL group to the next available claims handler.

This meant that the claims handlers had little time to familiarize themselves with a claim, typically giving little more than a cursory glance to the details surrounding the incident. In contrast, CM staff demonstrated some degree of claim ownership and hence it was a much better environment in which to ensure suspect claims were spotted. For example, CM staff typically had more in-depth knowledge of individual claims than NOL staff, and often recalled claim details from memory to the ethnographer. However, CM staff worked in teams, each team dealing with claims based on an alphabetical split around claimant surnames. Frequent changes in team membership meant that claim allocations were reshuffled across teams. This reduced familiarity with claims and disrupted ownership of claims. The company also had no formal mechanism to ensure feedback to staff about cases they had referred. In discussions with the researcher, staff often recalled suspicious cases but had no knowledge of the case outcome since the case had passed to a new team before a decision to pay or refer the claim for specialist investigation. Claims handlers appeared resigned to the fact that nothing would come of suspicions that they referred for further investigation. It seems likely, then, that feedback and ownership might also sustain staff motivation to detect and report fraud.

A third issue concerns the integration of fraud detection and investigation processes with the company's general claims-handling procedures. NOL staff worked from scripts to elicit claims information systematically from clients, but the scripts did not contain questions necessary to elicit information that might identify fraudulent claims. The requirement to remain logged onto the telephone systems and the need to move swiftly onto the next call meant that NOL staff often completed checklists of fraud indicators some time after a call was taken. Databases recording the insured's claims history might yield some information, but other critical information cannot be identified once a call has ended. Furthermore, to ensure swift claims settlement (e.g. on receipt of a solicitor's letter from a third party involved in an accident), claims handlers were often required to begin processing claims before they gained sufficient information to assess claims against fraud indicators. For example, a claims handler was observed completing a fraud indicator sheet based on a badly copied fax whilst another was observed completing a sheet based on only a letter from a third party expressing that they had been involved in an accident with an insured. Frequently, claims were reported by insurance brokers acting on behalf of the insured and they only had the information provided to them by the insured. Often under these circumstances, claims handlers had to make assumptions when completing the fraud indicator sheets. For example, an extract from the ethnography describes a claims handler assuming that the insured had left his keys in his vehicle yet the claims handler did not ask the insured about their keys.

The procedure for using fraud indicators used by claims handlers was also problematic. For example, whilst the fraud indicators focused claims handlers' attention on known fraud types, the checklist approach implicitly discouraged identification of novel classes of suspicious claim that fell outside the scope of the fraud indicators. On two occasions, we observed claims handlers who did not refer claims because they were unable to find reasons for referring a claim based on the fraud indicators, despite the case being clearly suspicious for additional reasons. For example, a claims handler had concerns that an insured had not disclosed a driving conviction at policy inception but did not refer the claim as it had only triggered one fraud indicator.

During our observations of the NOL group, no suspicious claims were identified purely by applying the fraud indicator checklist. In part, the problem stemmed from the fact that completing the fraud indicator checklist was implemented as a single step in the claims-

handling process: fraud indicator sheets were not updated when subsequent claim details came to light. Moreover, the company did not analyse the predictive ability of specific indicators to highlight fraud.

The ethnography revealed that, where suspect cases do get detected by Company A, this often results from the actions of external agents. Several professional sources are involved in the claims-handling process, such as loss adjusters, engineers, garages, and insurance brokers. Examples of external sources identifying suspect cases include engineers and garages reporting vehicle damage as inconsistent with accident circumstances described by the claimant, reporting damage that must have occurred prior to accident because of rust on dents and so forth, and also reporting that the vehicle would have been un-roadworthy prior to the accident (e.g. because of a lack of brake fluid in the braking system). A further example was of an insurance broker telephoning the CM group to report he was concerned that his client had lapsed payment on several insurance policies. Subsequent investigation of this client led to the discovery of fraud.

A major difficulty concerning the involvement of external agents was inadequate or inaccurate communication of claims information and suspicions between relevant parties. Loss adjusters frequently complained to us during the project that claims handlers provided only sparse claims information and did not communicate their suspicions. Their problem is exemplified by the following extract from the ethnography:

“A loss adjuster rang to ask if the case had been referred due to the presence of fraud indicators or another reason, and asked for driver details and a copy of the claim form. The person wanted to know was there any reason it was being investigated, only it was quite low value and she wanted to know if she was missing something.”

Furthermore, we observed instances where claims handlers failed to act upon or document suspicions provided by external agents. For example, an engineer's report was sent to NOL suggesting suspicious behaviour by a garage. There was also a note on an engineers report sent to CM saying that there was a problem with the insured's mobile number and some concerns over the validity of their purchase invoice. In both of these instances the claims handler failed to follow up these concerns. Information from external sources affords a useful opportunity for insurers to capitalize upon. However, this depends crucially on optimizing the processes and channels through which communications take place between claims handlers and external agents. In summary, it seems clear that the relationship between insurance companies and external agents (in particular loss adjusters) is crucial for effective fraud detection and investigation. Further research that we have undertaken has examined this relationship in detail, but consideration of the results of this work are beyond the scope of the present paper.

#### *The role of the claims handler*

Handling claims within NOL was characterized within the company as a low-level job, essentially equivalent to that of a telephone receptionist, a job that was repetitive, attracting low rates of pay and little training. As a consequence, NOL had the least experienced staff. Arguably, however, NOL is the best position at which to spot potentially suspect claims, since it minimizes the costs associated with investigation and allows questioning of clients prior to awareness that an investigation is in progress. On average, NOL staff had less than a year's experience with Company A, and many were unfamiliar with the insurance domain in general as well as in the specifics of fraudulent insurance activity. Young staff (often school

leavers on a gap year before university) lacked world knowledge about suspect information. For example, many did not possess insurance policies, own a car, or know the value of pieces of furniture. Knowledge limitations are likely, therefore, to preclude the detection of some classes of fraudulent claims such as financial exaggerations.

Claims handlers also appeared to operate under their own conception of fraud, which often did not correspond to the company view of fraud. Claims handlers readily discussed with our researcher “suspicious” cases that they had encountered, but they invariably stated that they had *never* detected fraud and did not come across fraud in their day-to-day activities. This paradox seems to reflect the fact that these individuals tended to define fraud as being restricted to large, high profile, and probably court-proven cases involving significant sums of money rather than encompassing cases such as an individual exaggerating a modest claim. Some staff stated that fraud wasn’t an aspect of their responsibility. Yet all of the claims handlers we interviewed accepted as their responsibility the company goal of making sure that the insured did not profit from an insurance claim beyond the proper value of the claim.

A common hypothesis in the insurance industry is that fraudsters are more likely than genuine claimants to complain and be aggressive on the telephone. Observations of NOL and CM groups indicated that the attitude of the insured affected how a claims handler responded. If the insured was co-operative and personable then claims handlers were likely to believe their story, perhaps even feeling sorry for them and attempting to be additionally helpful. In contrast, when an insured was aggressive or complaining, claims handlers were likely to see them as suspicious and take steps to try to undermine their claim. For example, we observed a claims handler conducting a search on the CUE database for details of the claimant’s insurance history, as an attempt to gather evidence to create a suspicion, solely because the claimant had been aggressive on the phone. This finding has two implications. First, if claimant’s manner is a good predictor of the fraudster profile, then claims handlers of all levels of experience already act upon it, suggesting that profiling technologies that identify inappropriate manner in callers are effectively redundant. Second, the relationship between the fraudster profile and aggressive manner might be an illusory correlation, the claimant’s attitude leading to greater vigilance and reactivity in the way the claims handler deals with the claim.

Our observations identified a widespread aptitude among experienced claims-handling staff at spotting anomalies in claims information. For example, a claims handler noticed that the insured had reported that both sets of car keys had been stolen, and yet they had returned a set of keys with the claim form as requested. Many anomalies were detected as a result of claims handlers’ knowledge and dispositions, deriving from familiarity with similar claims or personal beliefs relevant to the claim. Prior knowledge and beliefs typically revealed themselves as assumptions about the circumstances of the insured and the type of incident that took place. Our field notes record the following example from NOL, which we annotate (in italics) with apparent beliefs that underlie the claims handlers’ reasoning:

“A fairly inexperienced claims handler queries the personal-effects limit on a commercial vehicle policy because this person has had a digital camera stolen from his car. An experienced claims handler replies that it is £250, but then adds that there is a £50 excess for a broken window [*a belief-based assumption that the camera was stolen because it was in view*]. The inexperienced handler replies that there is no claim for a broken window because the camera was taken from the boot. The experienced claims handler then replies that it is odd that a camera has been stolen from the boot when there is no claim for any

damage to his vehicle [*evidence of an anomaly detection based on a belief that theft from the boot would necessitate forced entry and subsequent damage*]. She notes down the need to phone the broker and make further enquiries before the claim is authorized.”

This example illustrates the essentially opportunistic manner in which claims handlers detect anomalies. In this example, the inexperienced claims handler made an enquiry about the personal-effects limit that led the experienced claims handler to identify an anomaly. Further evidence of opportunistic detection of anomalies comes from observations of claims handlers, mainly those in the CM group, using their local geographical knowledge to detect anomalies. For example, one claims handler noticed that a picture presented as evidence of the ownership of an allegedly stolen vehicle was taken in her own street, the vehicle being parked outside a house at which criminals were known to operate. Another example concerned two claims handlers discussing a claim; one of the claims handlers happened to live in the locale of the recovery area and observed that the vehicle was recovered close to the insured's house when it had been stolen many miles from that location. The influence of local knowledge is interesting to observe, as increasingly insurance companies de-regionalize their claims operations. For example, a claims handler in Cardiff could be dealing with a claim that occurred in Leeds.

Notwithstanding evidence that claims handlers could identify anomalies, often they did not register such anomalies as problematic or suspicious, and instead continued to process the claim on-screen or put the claim file back into filing. For example, we observed a claims handler who was concerned that a claimant had sent in a large set of documents at the point of notification of loss; the handler explained that a claimant wouldn't normally know that the submission of such documents was required for the processing of their claim. Yet the handler failed to make any written note or to raise any query about this observation, despite also finding a MIAFTR match for the car being a previous total loss. This finding suggests that the focus of the problems that the industry has in dealing with fraud may not be the detection of fraud *per se*, but in the absence of procedures to deal with the anomalies that staff detect.

The ethnographer identified one team of claims handlers in the CM group whose members were observed to demonstrate a much higher rate of identified suspect cases compared to any other team. They were also observed to be more vigilant and thorough in dealing with claims. This team was responsible for dealing with claims for classic and cherished car policies. The team as a whole was more aware of fraud and had considerably better memories for cases than teams in other motor sections. A number of factors may explain their increased awareness. For example, the members of this team received fewer telephone calls than individuals in other departments, and they spent considerably longer on each claim file than was typical in others sections of the company. The team was also more cooperative when it came to discussing suspect cases and its members were generally more experienced in insurance and had more personal knowledge about cars than those in other departments. This specialist team demonstrated the interactive nature of factors such as time, vigilance, cooperative fraud detection, and experience, and the key role that such factors can play in determining fraud-detection capabilities.

We also observed inexperienced staff in the NOL group detecting anomalies, but this occurred less often than with experienced CM staff. Inexperienced staff tended not to possess what Clarke (1989, p. 5) refers to as the “occupational hazard” of suspicion. Instead, they tended to adopt what we refer to as a “framework of innocence” when interpreting claims information. That is, they treated claims as genuine from the outset.

Claims handlers in the CM group, on the other hand, were more likely to operate under a “framework of suspicion”, perhaps because they were often dealing with follow-on information requested to clear up uncertainties in the initial report of loss. Although a framework of innocence might hinder anomaly spotting, it is appropriate in that the majority of claims are genuine. In this sense, inexperience among NOL staff prevents unnecessary scrutiny of genuine claims, thereby reducing upset to genuine claimants. In our view, the adoption of differing frameworks for evaluating claims information at different stages of claims processing is an important part of a successful process for tackling fraud, since one must balance the benefits of detection against the costs of false positives. It is interesting, therefore, to see how, in assigning staff of different levels of experience to different stages in the process, the company implicitly embodied this shift in framework.

### *Technological issues*

The fraud-detection process relies heavily on accurate and comprehensive communication of claims information and suspicions, especially in situations where there is no case ownership. The claims-processing software used by NOL and CM groups was old and inflexible. They used two different systems: HUON, a claims management system designed for use on personal motor insurance claims; and I90, a similar system designed for use on commercial motor insurance claims. Both systems were effectively repositories for claims information, allowing documentation of all actions, communications and correspondence surrounding a claim. The marked difference between these two systems was the extent to which we observed evidence of claims handlers documenting anomalies. Extensive observations of staff processing claims using both types of system revealed no documentation of anomalies in HUON whilst we observed several instances of anomaly recording in I90. This discrepancy arose because of differences in the way claims handlers could add notes to each system. I90 had a single notes field, so claims handlers could see notes entered by themselves alongside those entered by others. In HUON, each note entailed a discrete entry, with only the first line of previous notes on-screen. The claims handler had to check a box next to any note to read it. From a fraud perspective, these notes play a vital role in communication between claims handlers. Requiring users to skim through all the notes before adding their own, as in I90, helped to ensure that anomalies were monitored and augmented. The same interface requirements may have also been the source of increased note-taking behaviour because scrolling would give claims handlers a sense of absence of information and would potentially encourage them to add a note when the existing records did not match their observations.

During the ethnographic study, the fraud unit in Company A provided some CM staff with access to the CUE and MIAFTR databases as a proactive move in tackling fraud. However, lack of training and backup support meant that CM staff often used ineffective search strategies when using these databases. CM staff tended to enter information in all available fields when constructing database queries. However, entering data in all search fields reduces the likelihood of a data match occurring. Experienced investigators tended to search using only a small subset of fields to maximize their search effectiveness, even when additional information was available. Claims handlers also struggled to interpret the information obtained from these databases, often interpreting a match returned from a query as identifying a fraudster. Information supplied by these databases, however, can only reveal the previous claims history of people. The data they reveal require careful interpretation, especially in the light of the many false positives generated by data entry errors.

*Comparison with Company B*

Company B has a strong customer-service focus that again seemed to be detrimental to its fraud-detection capabilities. Like Company A, the company emphasis on being proactive in claims handling, staff targets based on quantity and call performance, and lack of incentive for detecting fraud, inhibited fraud detection. Unlike Company A, claims handlers in Company B were, in theory, assigned to monitor individual claims throughout their progression, offering some degree of case ownership. However, in practice senior staff typically encouraged the claims handlers to circumvent the process and to deal with a customer's query themselves, thus offering speedy assistance rather than incurring processing delays that would arise from referring claims to assigned advisors.

There was no systematic fraud-detection process in place in the claims department of Company B. However, a number of experienced staff was responsible for dealing with, and advising upon, suspicious claims identified by claims handlers. These staff had been selected because they had shown an interest in fraud detection. Their role was to act as a referral point for fraud issues arising from the claims department. These representatives then fed this information to the fraud department, a team of five in-house fraud investigators. These investigators were relatively young and had on average one year's fraud experience. Two of them had been recently promoted from the claims department. This formal process of referral of suspicions promoted the documentation and communication of suspicions. However, the process relied heavily on claims handlers reporting suspect cases, which they were often reluctant to do for the reasons described earlier in this section.

The company focused its fraud-detection efforts in the fraud department. Here all new policies and claims were checked against databases of fraudsters and an in-house database of fraud intelligence was maintained. This process appeared effective at spotting anomalies and patterns in claims data. However, investigators often failed to interpret anomalies and patterns as being potentially suspicious. Nevertheless, we observed the process identify several fraudulent cases.

As in Company A, many suspect cases in Company B were associated with anomalies reported by external agents. We observed only one example of a claims handler identifying a suspect case, when they recognized a forged MOT certificate. In this case, Company B provided feedback to the claims handler about the outcome of their suspicions. A fraud investigator confirmed that the MOT was indeed forged and rang the claims handler to notify them of this outcome. Despite this example of feedback, the fraud representatives in the claims department complained that they rarely received feedback on the outcomes of suspect cases.

The software technology used by Company B was more flexible in relation to detecting fraud than that used by Company A, specifically in incorporating a useful preventative measure. The system allowed the marking of policies of potential or known fraudsters to prevent policy renewal. However, this process relied on human operatives marking the policies. We observed one instance where the marking system was overlooked: a policy had been voided in 1998, but no marker was placed on the system. In May 2002, the company cancelled another policy of the insured due to non-payment, but again no marker was placed. In July 2002, the insured took out yet another policy and three days later, they submitted a claim that Company B had to honour. Company B also employed other technologies such as CUE and MIAFTR and these were available for use solely by the fraud investigators. During the period of observation, however, none of the fraud investigators used these databases.

In summary, both companies had strong organizational objectives that appeared incongruent with the process of fraud detection. The noticeable difference between companies was in the fraud processes that were employed. Company B had a more high-profile fraud initiative within the organization but it was barely visible in the claims department. Company A, in contrast, had a formal fraud-detection mechanism in place at the front end of the claims process. Company B had also taken some preventative measures in the fight to tackle fraud, whilst Company A was more reactive to fraud and dealt with it when it arose. Despite these differences in work practices, both companies showed similar low levels of fraud detection (as identified by a mismatch between the levels of fraud detection observed, compared to industry estimates of presence of fraudulent activity) and a heavy reliance on external sources of information and staff expertise.

## **Discussion**

The ethnographic study of ongoing claims-handling processes in two major companies that we report in this paper allows us to synthesize an understanding of the limitations that exist on capabilities for detecting insurance fraud. Organizational factors such as high customer-service standards, speed, efficiency, proactivity, staff assessment and productivity targets all emerged as variables that dominate the structure and efficacy of the claims and fraud processes adopted by companies. These factors contribute to a culture of low levels of training and a lack of feedback and case ownership that discourage staff from reporting potentially fraudulent claims. Moreover, processes put in place to encourage fraud detection, using procedures based around fraud indicators, may actively inhibit the detection of new classes of fraud. Also, old and inflexible software systems were shown to be detrimental to fraud detection, in failing to support either the elicitation of relevant information or the documentation and communication of suspicions.

Some of our observations seem to confound assumptions implicit in the development of novel forensic and data-mining technologies. Our observations suggest that claims handlers are adept at detecting novel anomalies, and are quite capable of responding when the manner of a claimant is inappropriate to them. This raises the question as to whether new technologies that aim to detect more anomalies and recognize fraudster characteristics from interviews and speech profiling are addressing the right target. Both NOL and CM staff, despite their differences in experience and knowledge, appeared capable of identifying anomalies, but lacked the organizational processes and technological support systems to develop anomalies into testable suspicions. It was additionally observed that data-mining technologies would be difficult to implement in companies who use paper claim forms, as additional data entry would be required. Likewise, it would be impossible for companies who use brokers as the point of notification of a claim to employ voice stress analysis techniques.

None of the companies we observed employed forensic techniques for claims-handling staff, although one company has since reported to us that they are implementing investigative psychology in their claims-handling process. One of the companies did, however, use a data-mining tool in its investigative department. Over the course of three days the ethnographer observed the performance of the system and the investigator interpreting the system output. Each day the system would match the hundreds and thousands of new policy and claims information against its extensive database of information and would throw up thousands of matched data items for the investigator to interpret. However, of these thousands of matched items only 25 appeared to be suspect by

initial inspection by the investigator and of those only one was eventually considered to be suspicious enough for further investigation. There appeared to be considerable redundant information in matched data items and interpretation of matched data items as suspicious required considerable fraud knowledge on the part of the staff. This again suggests that detection of anomalies is not the issue but rather what you do with the information that is important.

In terms of future developments, it would appear difficult for companies to change rapidly either their technological systems or their organizational objectives. We propose, however, that identifying how organizational and technological factors affect fraud detection can facilitate a better understanding of how to implement fraud-detection practices into revised claims procedures. For example, the workings of the specialist team in Company A offer a useful insight into best practise in how to improve fraud-detection methods.

This research highlights some negative aspects of current fraud-detection practices, but also indicates important opportunities to build on. With increased training and organizational support and through the introduction of appropriate supporting software technology, companies might improve their fraud-detection capabilities. We offer six main recommendations to achieve these aims, though implementation will depend on company policy:

1. To offer incentives and remove disincentives to staff in detecting and reporting anomalies. For example, call rate measures might be adjusted to take into account anomaly detection and documentation so that staff dealing with suspect cases would not be penalized for doing so.
2. To develop software and processes that support the documentation and communication of anomalies identified by claims handlers and by external agents, to enable insurance companies to capitalize upon the natural skill that all people seem to have in detecting anomalies. For example, software systems could be developed using web-based interfaces that facilitate the sharing of case notes across multiple sites.
3. To facilitate a degree of ownership of claims, coupled with the provision of feedback on case outcomes, to all staff involved in the handling of a fraudulent case, and to use this feedback to refine the fraud indicators given to staff.
4. To provide increased, and more regular, training opportunities for claims-handling staff.
5. To encourage better use of industry databases and better training for effective use of these databases. For example, outlining effective search strategies.
6. To develop organizational processes that properly integrate fraud-detection methods with general claims handling, particularly recognizing that fraud detection needs to occur iteratively throughout the claims processing cycle. At present, fraud screening takes place only when the initial claims information is first given to the claims handler.

Another aspect of the current research project has been to develop software technologies that implement these recommendations. This research is discussed further in Ormerod et al. (2003). We have also conducted a subsequent ethnographic study that focuses on expert fraud investigators dealing with claims that have been detected. The software systems we have developed mirror the kinds of expert cognitive processes used by fraud investigators to develop their suspicions, and push these processes towards less experienced staff.

A key distinction between our research and the approach taken by other researchers is our focus upon occupational rather than forensic studies of the fraud domain. Forensic

approaches are extremely valuable, but a focus upon the process of fraud handling is, we believe, an important complement to them. In particular, it is important to assess the degree of match between the processes used for detection of insurance fraud and the assumptions that exist concerning the nature of fraud and fraudsters. An ethnographic approach enabled us to examine this *in situ*. We acknowledge that concerns are sometimes voiced about the use of ethnographic approaches in behavioural research. For example, questions have been raised about the lack of control over factors that are investigated and the validity of the resulting data (see Ball & Ormerod, 2000b). Such concerns may limit the implications that can be drawn from ethnographic studies, but we believe that such limitations are traded off in the present research against the benefits that derive from using a methodological approach that optimizes the investigation of the reality of claims handling and that also takes account of organizational factors. Thus, our conclusions reflect the realities of contextualized fraud-detection practices. Nevertheless, in an effort to extend our research to address the aforementioned criticisms we are currently pursuing traditional experimental studies to validate our research results in a more controlled environment. To conclude, we believe that the present research is both timely and important; a clear applied benefit relates to the potential for this research to provide the insurance industry with a better understanding of the requirements of claims-handling staff in terms of areas that need support through training, organizational and process changes, and software development.

## Acknowledgements

The Frisc project is supported by the EPSRC/DTI Management of Information initiative, No. GR/R02900/01. We thank our project partners, UK insurance companies and loss adjusters for assistance in the ethnographic studies.

## References

- Anon (n.d.). Fraudscape – What is it? Retrieved 8 October 2003 from <http://www.fraudscape.co.uk/uk/fraudfolder/fraudhtml/whatf.html>.
- Association of British Insurers (2001). News release 18 October 2001. [www.abi.org.uk/newsreleases](http://www.abi.org.uk/newsreleases).
- Anderson, R. J. (1994). Representations and requirements: The value of ethnography in system design. *Human-Computer Interaction*, 9, 151–182.
- Ball, L. J., & Ormerod, T. C. (2000a). Applying ethnography in the analysis and support of expertise in engineering design. *Design Studies*, 21, 403–421.
- Ball, L. J., & Ormerod, T. C. (2000b). Putting ethnography to work: The case for a cognitive ethnography of design. *International Journal of Human-Computer Studies*, 53, 147–168.
- Bentley, R., Hughes, J. A., Randall, D., Rodden, T., Sawyer, P., Shapiro, D., et al. (1992). Ethnographically-informed systems design for air-traffic control. In *Proceedings of the Fourth ACM Conference on Computer-Supported Cooperative Work – CSCW '92* (pp. 123–129). New York: ACM Press.
- Clarke, M. (1989). Insurance fraud. *British Journal of Criminology*, 29, 1–20.
- Clarke, M. (1990). The control of insurance fraud: A comparative view. *British Journal of Criminology*, 30, 1–23.
- Crime and Fraud Prevention Bureau (2000). *Annual report*. Association of British Insurers. [www.abi.org.uk](http://www.abi.org.uk)
- Dodd, N. J. (1998). Insurance claims fraud: Applying psychology to the reduction of insurance claims fraud. *Insurance Trends*, 18, 11–16.
- Doig, A., Jones, B., & Wait, B. (1999). The insurance industry response to fraud. *Security Journal*, 12, 19–30.
- Dunham, M. H. (2003). *Data mining: Introductory and advanced topics*. Harlow, UK: Prentice Hall.
- Forsythe, D. E. (1995). Using ethnography in the design of an explanation system. *Expert Systems with Applications*, 8, 403–417.
- Gill, K. M., Woolley, K. A., & Gill, M. (1994). Insurance fraud: The business as a victim. In M. Gill (Ed.), *Crime at work, Vol 1*. Leicester: Perpetuity Press.

- Horvath, F. (1982). Detecting deception: The promise and the reality of voice stress analysis. *Journal of Forensic Sciences*, 27, 340–351.
- Hughes, J. A., King, V., Rodden, T., & Andersen, H. (1994). Moving out from the control room: Ethnography in system design. In *Transcending boundaries: Proceedings of the Fifth ACM Conference on Computer Supported Cooperative Work – CSCW '94* (pp. 429–439). New York: ACM Press.
- Hughes, J. A., O'Brien, J., Rodden, T., & Rouncefield, M. (1997). Designing with ethnography: A presentation framework for design. In *Proceedings of the ACM Symposium on Designing Interactive Systems – DIS '97* (pp. 147–159). New York: ACM Press.
- Hughes, J. A., Sommerville, I., & Bentley, R. (1993). Designing with ethnography: Making work visible. *Interacting with Computers*, 5, 239–253.
- Hunter Product Information (n.d.). Retrieved 8 October 2003 from <http://www.mclsoftware.co.uk/details.html>.
- Kebbell, M. R., Milne, R., & Wagstaff, G. F. (1998). The cognitive interview: A survey of its forensic effectiveness. *Psychology, Crime & Law*, 5, 101–115.
- Litton, R. (1990). Fraud and the insurance industry: Why don't they do something about it, then? *International Journal of Risk Security and Crime Prevention*, 3, 193–205.
- Litton, R. (1998). Fraud and the insurance industry: Why don't they do something about it, then? *International Journal of Risk Security and Crime Prevention*, 3, 193–205.
- Ormerod, T. C., Morley, N. J., Ball, L. J., Langley, C., & Spencer, C. (2003). Using ethnography to design a Mass Detection Tool (MDT) for the early discovery of insurance fraud. Paper presented at CHI 2003, Fort Lauderdale, Florida, USA.
- Schneiderman, B. (1998). *Designing the user interface: Strategies for effective human–computer interaction*, 3rd edn. Harlow, UK: Addison-Wesley.
- Steed, A. (2003). Insurers to trial lie test for fraud. *The Daily Telegraph*, 15 August 2003.
- Suchman, L. A. (1987). *Plans and situated action: The problem of human–machine communication*. Cambridge: Cambridge University Press.
- Viller, S., & Sommerville, I. (2000). Ethnographically informed analysis of software engineers. *International Journal of Human–Computer Studies*, 53, 169–196.