11

Investigations

It used to be a good hotel, but that proves nothing—I used to be a good boy.

Mark Twain, author

The first hotel security personnel were referred to as "detectives" for a reason. Losses are recovered and prevented with investigations. You just cannot operate a hospitality Security Department without investigations. Most incidents require some follow-up and you need some behind-the-scenes people turning over stones to see what is really happening on your property.

PRELIMINARY INVESTIGATIONS

Most of this book focuses on prevention and being proactive to maintain a safe, secure, and comfortable environment for everyone. In this chapter, we focus on the reactionary side of the business. Response is probably the most visible aspect of the Security Department and likely the place where we can make the best impression on our guests even though most of these types of interactions are negative. Fortunately, if done properly, a good security officer, following good procedures, can turn this negative into a positive.

The purpose of the preliminary investigation is to gather and document as much information as possible while the guest is still present, or while the incident is still "fresh." Every incident has some sort of investigation, even if the responding officer at the scene concludes that investigation. We will start with that initial response, gather evidence, and then begin the investigation itself.

Response to Calls

The investigation of any incident begins as soon as the first officer arrives on scene. The officer has already begun the process as she approaches and mentally records the scene. This recording includes what the scene entails: persons present, their actions, placement of objects, condition of the area, weather, lighting, etc. It is up to you to train the officer to memorize and document these important pieces of data. Granted, not every piece of data

is relevant to every scene, but rather than try to distinguish in advance which ones are, it is better to go for the entire thing. Sorting through too much information is better than later wishing that you had it. Providing the officer with tools will allow her to do this preliminary investigation completely and efficiently.

Training

Training, as usual, is the first step. Start with an awareness of the goal of the investigation. Most officers do not take the time to be as detailed and thorough as they could because they do not understand the criticality of the investigation. It has to be explained to them that even though maybe 1 of 100 of these investigations do little more than get filed away, that one could cost the company hundreds of thousands or millions of dollars. This is not an exaggeration. There are many cases throughout this book that could be used for this training.

Once the awareness is engrained, technical training must be provided. (Training is covered in more detail in Chapter 6.) Officers should be shown to document everything as they see it upon arrival. If possible—if it is not an emergency—the first officer should look carefully at the overall scene. In a guest room, he should note the condition of the door, the items in the bathroom, signs of struggle or accident, other persons present, etc. A camera is the best way to document and can be a good way to jog an officer's memory later, but notes should still be taken. The camera will not capture sounds, verbal statements, smells, and even lighting conditions. Taking notes is not that simple. It is difficult for anyone to know what he or she should write. As mentioned previously, just write down everything. It helps to have another officer who can take statements and discuss the situation with the guest while the first officer concentrates on documentation.

Photography

Anything that supports the statements should be photographed. Anything that contradicts the story also should be photographed. In other words, the entire scene must be photographed. Start with an overview of the scene. This shot should put the location into context. The second shot is generally an overview of the specific location, showing placement of objects. Then take individual shots of each object from different angles. Close-ups should be taken if possible. A full and facial shot of everyone involved is important because the investigator will use these to identify people on video.

Interview

Once the scene is "preserved," at least in memory and in photos, the next step is to reconstruct what happened. This is accomplished by first obtaining a verbal account from the "victim" and then from any witnesses. Allow them to verbalize the story, separately if possible, and before they write it down. As they recount their experiences, let them speak uninterrupted as you take notes. After the verbal statement is given, ask questions to clarify or understand. Then repeat it back from your notes. "So you used your key, walked in the room, and saw the suitcase lying upside down on the floor right about here." If they then change the story, note the change. Then have them write the statement. Once you

have the statement, compare their verbal and written statements for clarification. "You told me that you used your key to open the door, but your wife said you lost your key and used hers." (We are not interrogating, just asking for clarification.) Once you have their statements down, compare the story with the evidence. "You said the suitcase was upside down on the floor, but it is now on the bed." This goes on until we have his story, her story, the maid's story, and our story (what we saw). These will be put together in the report.

Evidence

Evidence is everything that supports or disproves the incident. Your legal counsel has to decide what physical evidence she wants you to gather and retain. The police handle criminal evidence. Our evidence refers mostly to accidents, noncriminal incidents, or even criminal incidents if the police did not want the case. Included in these categories are stools from which guests fall, broken glasses in which their mouths were cut, or a bottle of cleaning fluid that burned their eyes. If your counsel finds these items unnecessary, then do not save them, because once you do, you are stuck with them.

Gathering evidence is a process that has to be taken seriously. Handling must be done in a way that does not damage or alter it. Packaging should be done so as not to further damage or contaminate the item, and it must be sealed so there is no question as to whether it was tampered with. Storage must be secured and access limited to one person, such as the investigator.

There may be external items to be retained, such as video, computer data, reports, lock interrogations, and so forth. These must be labeled and preserved with the report.

Once the statements, photographs, and evidence are gathered, the preliminary investigation is complete.

REPORT WRITING

A report is simply the documentation of an incident to preserve the information for later use. Reports may be seen by supervisors, department heads, police, lawyers, prosecutors, juries, and judges. This needs to be stressed to the report writer so that like the preliminary investigation, the report is thorough, detailed, and accurate. Report writing is arguably one of the most important functions of the Security Department, so even though you have given and received training on it, I am going to go over the important stuff.

Officers should be hired and trained with the objective that they will write reports based on incidents that they see. Having supervisors or specialists write the reports works for some, but is awkward. It is difficult to write a report in the first person if one is not at the scene. Supervisors are trained and paid to take more responsibilities than this front-line duty, so this process is inefficient. Hiring officers who can already write is a big help.

Format

Whether you use report-writing software, a word processor, or write by hand, these elements are standard. First is the statistical stuff, and second is the narrative. Last are the attachments.

Report Data

This statistical information is placed in a certain order and format for several reasons. First, it allows the reader to discern the basics without reading through an entire narrative. Anyone can pick up Page 1 and see who was involved, what the loss or injury was, and what the value was. Second, it makes the job of the data entry person easier. If you have to enter data manually, these fill-in boxes make it much faster for the clerk and reduce errors. Third, including all of this information in a narrative format makes it cluttered and difficult to read.

Almost every incident has photos. We already discussed how and where to take them; now they have to be documented in the report. The photos should be listed before the narrative with a number that corresponds to the photo or file name. A brief description, name of photographer, location, date, and time taken should be included in this list.

Video is also included in many reports. You may choose to have your investigator review video for the officer, but the reporting officer should really do it. This helps the officer put the story together and saves the investigator time. It also ensures the video is pulled and saved before it goes stale or is recorded over. In the report, video should be listed similar to the photos, and in the narrative a summary of what the officer saw on the video. This is included in the narrative because not everyone is going to have time or even the original video to review, so the narrative will help them decide if they even need to bother looking at it.

Narrative

This part is much easier than everyone makes it out to be. The narrative simply tells a story, in chronological order of what the writer did from start to finish. It should be done in the first person (use "I" instead of "Officer Jones" or "This officer"). These are outdated forms of writing and are difficult for a layperson (like on a jury) to read and understand.

The narrative starts at the beginning (from the writer's point of view): On this date at this time, I was dispatched to . . . Or: On this date at this time, I saw. . . . As the narrative continues, it is easiest to tell the story from the eyes of the officer as it happened. "When I arrived I saw this, I did this, and this person was doing this and then I did this. Mr. Guest said that this happened, then I spoke to Miss Customer and she told me this happened." On and on it goes until the officer leaves the scene. Then she continues writing whatever follow-up she did—gathering statements, room information, lock interrogation, etc.

Corrections

Officers should correct their own reports by proofreading them. Spell check is a good tool, but the wording and grammar should be their own. Using big words or words they don't understand will cause problems later if they are deposed. Their own wording should be used as long as it is accurate. I am not saying to use slang, profanity, or gibberish, but it is not necessary and does not sound like normal conversation to use words like "approximately" and "expedited" when "about" and "hurried" will do.

Hint

Officers who are self-conscious about their writing ability will sweat, stall, and struggle through this process. Ask them to stop writing and tell you what they did on the call. They will likely tell you a story like the one I related before. Perfect. Now write exactly what you just told me. They are likely stuck on the big words and what they think we want to see. When it dawns on them that a story in their own words is what we want, it makes it as easy as writing in a journal or diary. When they get to that part, we just fine-tune the edges with such things as photos, video review, etc.

Attachments

Numerous documents having relevance to the report should be attached directly to it. Do not presume that other departments will hold the info for you or that it will be attached later. Some attachments that are common in hotel reports are the statements from guests and victims, the room folio, lock interrogation report, reports from housekeepers and engineers, and any other paper document that is necessary to support the report.

The written report with supporting video, photos, statements, and other evidence concludes the preliminary investigation. I hope that you have an investigator who can follow-up on it if necessary.

INVESTIGATIONS

Investigations in the Hospitality industry are usually considered somewhat reactionary, where the investigator follows up on certain reports to "solve" them. This is only partially true. If you limit your investigators to follow-ups, you are severely limiting their capabilities. These are some of your most well-trained, highly skilled employees and their talents can be put to work in other ways that benefit the property. In this chapter, we will not only discuss how to recover assets, but also how investigators compile data, analyze it, and enforce vulnerabilities.

Unlike police detectives, the objective of a hotel investigator is not to prove (or solve) a crime, but to protect (or recover) assets. Call this your "Loss Recovery" unit to keep the focus on the objective. Recovery, in security, is most often accomplished through report follow-up. In most cases, security officers generate reports. (In some cases, investigators will initiate a report from information they received directly. This is discussed later.)

Report Follow-Up

It is the investigator's role to review reports for thoroughness, extract statistics, and monitor incident trends. He should not be looking for grammar, punctuation, and sentence structure (that should be done by a supervisor), but needs to flag reports that are lacking in information he might need for an investigation. If there is video missing or a witness statement that was not included, these need to be attended to immediately even if the investigation has not started.

The investigator extracts statistics that will be important for crime analysis and risk assessments (later in this chapter) on all reports. As for follow-up, this is done on those reports that meet certain thresholds set up in advance with the director of security. Thresholds (or triggers) are established based on the staffing levels—how many investigators to handle how many incidents—and what reports are worth solving. If there were 10 missing property reports per week and only one investigator, you might raise the loss amount up to reduce the number of reports to investigate. On the other hand, if your claims representative were going to automatically pay claims less than $50, it would not be worth investigating values less than that. This is not to say that these losses are ignored. You will still track them to see where they fall in your Risk Assessment and to see if there are any commonalities, such as the same valet attendant or certain room numbers and so forth.

Thresholds may get more complicated depending on whether there is enough evidence to conduct an investigation, the workload of the investigator, if the suspect is an employee, if there is liability on the hotel, etc. Whatever the thresholds are, they should be documented so the investigator may apply each report he sees to the criteria and make a quick decision to close the case or leave it open. There also should be a regular meeting, perhaps weekly, between the investigator and the Director to discuss the cases and determine whether they should be investigated based on workload, other investigations that have occurred, or input from the General Manager or Risk Manager. Triggers are discussed in further detail later in this chapter.

Some incidents will be investigated every time, such as sexual harassment, employee theft, discriminatory offense, or law enforcement (criminal) involvement. Set those criteria in advance as well or handle them on a case-by-case basis so they are not overlooked. Types of investigations vary depending on the incident, so we will go through each type you are likely to encounter at your property.

You will likely be investigating five types of incidents:

Internal—Any incident involving an employee as the suspect (offender) or as the victim (complainant). This would include most property losses, damage, employee theft, and guest complaints.

Criminal—Any incident where the police or a law enforcement agency will bring charges against an employee or guest.

Accident—Guest accidents and injuries. This includes food poisoning claims, bed bugs, etc.

Workers' Comp—Employees injured in the line of duty and work-related illnesses. Food poisoning, carpal tunnel, second-hand smoke, etc.

Personnel—Incidents involving employee misconduct, such as sexual harassment, intoxicated on duty, and employee complaints.

The investigator will have to determine the type of incident, who will do the investigation, and the type of investigation. These types are based on the expected outcome:

Personnel—Might result in disciplinary action or term
Criminal—Could result in criminal charges
Workers' Comp—May result in claim denial
Guest claim—Determine fault of company

Personnel Investigations

The first consideration of a personnel investigation is who will do it. Many HR departments prefer to conduct their own investigations. This is fine, but make sure their investigators are trained in interviewing skills. Smaller organizations hire an outside investigator to conduct these. I prefer Security to do all investigations, not only because of the training they have, but because it is a "third party," which allows HR to make an unbiased decision. A second consideration is consistency and fairness among all employees. HR and some department heads will think they have an easy case (two or more witnesses saw misconduct) and will make a termination decision without an investigation. This is often not a problem, but this employee may have a case against the company if he can show you required a full investigation by Security with other employees and not him. On the other hand, the employee who is terminated after a thorough investigation with interviews and an interrogation may claim discrimination because the other employee was not subjected to the same treatment. Establish a system with your HR Department that puts all employees through the same type of investigation so your actions are perceived as fair.

In 2008, a restaurant worker, who had been sexually harassed by her boss, sued the restaurant for hostile working environment. The restaurant had completed the investigation within two days of the first report and fired the harassing boss. The court ruled in favor of the restaurant because they had taken thorough and quick action against the offending supervisor.

A consistently enforced policy and thorough investigations can help a company defend itself from these types of suits. Sloppy or slow investigations can lead the victims to believe that management does not buy into their own policies or that management is trying to cover for its unacceptable behavior.

Written statements are usually the first step in any investigation. Statements should be obtained from all parties in the incident. This is a common way for the investigator to receive the investigation. A manager hands him the statements and he does the rest. (Don't complain about this—the less done on your behalf, the better.) The initial statements will likely be from the "victim" or the one making the complaint. There also may be a "suspect" or offender statement. If these statements have not been written yet, do not obtain them. A good interviewer will get better information verbally and nail it down with the written statement afterward.

It is common, in our culturally diverse environment, to get statements written in a foreign language. Do not trust other employees to translate this for you. Friends and co-workers will not provide an accurate translation and will insert their own opinion of what they think the victim should have written. Have a prearranged Security or Human Resources employee to do this for you.

Verbal translations should be handled in the same way. Do not use the employee's supervisor or co-worker to translate for you. You will need a qualified translator—at least an unbiased one.

The next step in an investigation is to gather evidence. Evidence includes any item or piece of information that will prove or disprove any part of the incident. This may be video, email, personnel files, policy excerpts, and prior cases. Each of these items needs to reviewed, documented, and filed with the report.

Video may or may not show the incident as described, but it also may be used to prove that the incident did not happen as alleged. It is useful as well for identifying witnesses that can be interviewed and to prove witnesses actually saw anything at all.

Email and other computer data are invaluable in many types of cases. This information should be saved in its data form and on paper to include with the report. Do not rely on the department or Information Technology (IT) to archive this for you. This data can be easily misplaced and your case lost.

Personnel files may or may not show previous related incidents, such as a pattern of behavior or a tendency to make false reports. They also may contain policy memos that were signed by the employee prohibiting that behavior.

Policy excerpts are necessary to justify your case. If you are investigating sexual harassment, include that policy to show what your case is proving.

At this point in your investigation, having reviewed the available evidence and statements, it is time for a management conference. This is usually between HR, the department involved, and the investigator. This is a chance for everyone to understand how much proof will be needed (this is discussed later) and what type of proof—a confession, two corroborating accounts, certain wording in an email—and what the expected outcome will be—termination, suspension, discipline, remedial training, etc. The investigator can also pick up some negotiating tools to use in his interrogation. "If you admit to this and undergo some counseling, I might be able to get you off with just a suspension."

Interview

An interview is simply asking and answering questions. Notes are taken, but it should be audio and video recorded with the camera facing the subject. There are interviewing and interrogation skills that require specialized training and every person who conducts these processes should have that training. We will touch on some of it, but this chapter does not replace that training and a lot of practice.

Victim

We usually start with the victim first. This is not vital, but it just makes more sense to get the original complaint directly from the complainant so you understand exactly what you are investigating. The interview is nonconfrontational and a chance to get the victim's side of the story. Just as was done in the preliminary investigation, questions are asked and answers repeated to clarify. Note: I have seen many company investigators perform this initial interview like an interrogation, accusing the employee of causing the problem, and deriding them for wasting his time. You do not want this type of rapport with employees. Let them know you are trustworthy and sympathetic. This will earn their respect and trust, and word will travel quickly that you are one they can go to for help or to report someone else's misconduct.

During the interview, the investigator is doing several things. First, he analyzes the written statement and compares it to the statements made verbally. Second, he examines body language. This is not quite the same as what you see on TV. The concept is to determine someone's truth-telling style by noting their body language and mannerisms when they are telling the truth, then comparing that style to answers given later during questioning. Third, he is deciding what questions to ask to extract more information on certain points that arise.

During the interview, the investigator also will introduce questions that arose from reviewing evidence. You said it happened here, but the video shows it happened elsewhere; tell me more about that. Your statement says that there was nobody else around, but an employee told me she was there the entire time and saw nothing; tell me more about that. Once again, there is some great comprehensive training available on this topic and it is highly recommended.

In conclusion, always tell everyone involved in an interview two things: (1) false accusations or false statements and refusal to cooperate with an internal investigation can result in termination, and (2) the interview and investigation are confidential and revealing the content thereof is a violation of policy.

Witnesses

Witness interviews are handled the same as the victim interview. Either their story will corroborate the victim or it will not, so you will need to delve into those conflicts. They may reveal important details that the victim left out. A witness can turn an investigation upside down, revealing a conspiracy to get the suspect in trouble, so keep an open mind and cull the facts. Witnesses should be admonished just as the victim was on disclosure and cooperation.

Nonwitnesses

You find these people without the help of the victim. A nonwitness is someone who was at the scene, but says nothing happened. These people can also reveal a conspiracy and have no motive to lie.

Character Witness

A character witness is someone who can vouch for the validity of the incident or the history of any one of the subjects in the investigation. They may be able to tell you if the two employees had a previous relationship if you are investigating domestic violence or sexual harassment. They may be able to tell you about their financial status if you are investigating an embezzlement case. Although they may not have witnessed any misconduct or an actual incident, their historical information may be relevant.

Suspect Employee

The last person to be interviewed (at least in the first round) is the suspect or the accused employee. If the employee has not yet written a statement, it is better to hold off until

the end of the interview. The reason for your interview is to get their side of the story. So, this interview should start out and remain friendly. The interviewer needs to build some trust and some integrity by reminding the employee that he is just doing his job, just wants the truth, wants the employee's side of the story, and may be the only person who can help him.

The employee should tell the story uninterrupted. During this time, notes are taken with careful attention to truth-telling style; gaps in mental time line, at which points in the story the mannerisms change, parts of the story that do not match; and parts of the story that are left out from the witnesses' or victim's story.

The truth-telling style was explained briefly before, and I cannot stress enough how important it is to have extensive training in these techniques. For the sake of the Security Director who needs to know what his investigator is doing in those interviews, I am summarizing it here. The interviewer pays close attention to the subject's telling of the story. It is better to have him start at the beginning of the workday and tell what he did from the moment he arrived on property that day. This gives a chance to identify the subject's truth-telling style. This style is displayed as he tells the truthful part of his day (where he parked, what he had for lunch, etc.). The interviewer notes his body movements, posture, facial expressions, etc.

As the dialog gets to the point of the alleged incident, we watch for changes in the body language, voice inflection, and so forth. These may indicate lies. We also listen for gaps in the timeline. There may be much detail as he recounts each hour of his workday, then breezes through the 15 minutes when he was in the storeroom drinking beer. It is more difficult to recall a lie, so people tend to leave out detail so they are not caught up in the lie. Once again, this may be an indicator, but it will be worth more investigation.

When he finishes his story, the interviewer goes back to the areas of concern. Whether it was a gap in the timeline, a different body language, or a difference between his story and the victim's, probe that area and repeat back what he said and say, "Tell me more about that." Do not tell him which part interested you; just ask him to talk more. This is done several times, continually narrowing him down or leading him through a complicated lie that he cannot get out of and that you know is not true.

Once this process is concluded, there should be some idea in the investigator's mind of whether the subject was being truthful. That is when you have him write his statement. This often puts him at ease that he is out of trouble because you could not get anything out of him. Do not prompt the statement; just say you need him to write everything that happened between 3 and 4 p.m. or everything he did in the storeroom up until he went to his locker.

Postinterview Conference

At this point, there is a pause in the investigation as the investigator reviews his findings. He either knows the employee is "guilty" or has learned new information that needs to be checked. If the latter is the case, the investigator goes back to evidence or more interviews until he has resolved all doubts or questions. If the investigator has already reached his conclusion, he will need to consult with his director, the HR director, and possibly the department head. This conference is used to review all the findings and determine the

next steps. (See "Burden of Proof" later in this chapter.) Someone will decide if there is enough evidence to stop the investigation and issue discipline or termination, or whether it will go unresolved with no discipline. It may be determined that everyone believes he did the act of which he is accused, but they want a confession. This is done through an interrogation.

Interrogation

The interrogation is somewhat different from an interview, and only necessary if there is not enough evidence. To begin an interrogation, the interviewer knows the subject is guilty, but does not have enough evidence. A confession is the goal of an interrogation. The interviewer does almost all of the talking and spends some time telling the subject how much evidence he has against him—statements, video, witnesses—he just wants to know why the person did it. Or he just wants to recover the money, or some other secondary concern. This takes some time to engrain in the subject's mind that guilt is no longer a doubt while he will deny it. Good interrogators use several styles to achieve the confession. They may use guilt, such as "What is your family going to think?" or they may be empathetic, "I know you just needed the money to feed your kids. I might have done the same thing in your position." Or, they may try promising them leniency, "If you just tell me how you did it, I can talk to my boss and maybe we won't press charges." There are many techniques and you may have to use them all for hours until the subject finally sees no way out.

A California employee of a large manufacturing company was called into the office and accused of theft of company parts. He was forced to drive the investigators to his home and submit to a search for the missing parts. The man sued for false imprisonment and invasion of privacy and was awarded $214,000.

Investigators have no authority to search a person and his property without consent. Care should be taken not to hold someone against his will and certainly not to physically force him to do anything. During an investigative interview, the only authority an investigator has is over the employee's employment.

Resignation versus Termination

Many companies will accept a resignation in lieu of an employee being terminated. HR Directors prefer this for many reasons. One is that their unemployment insurance may not have to pay on a resignation. This is hardly true anymore because employees can claim they resigned under duress. Two is that they believe they will save time and money if the employee decides to challenge his termination with a labor agency. This is also no longer applicable for the same reason. Three is that they are not comfortable with the evidence provided. It is generally not up to Security to make this decision or to accept a resignation. Whatever your HR Department decides, make sure your investigation is complete and accurate and includes all of the evidence even if you think you will not need it.

In 2010, a warehouse worker at a Connecticut beer distributor was being questioned about stolen beer. Investigators showed him video of the theft and offered to let him resign. The man calmly refused, asked to use the restroom, and came out with a handgun he had hidden in his lunch box. Nine people died.

Investigators should remain calm and friendly, but never let their guard down despite an employee's demeanor. This situation was avoidable and may have been prevented with some of the policies discussed in Chapter 7.

Conclusion

Remember that confessions are not necessary to prove or resolve your case. Later we will talk about the burden of proof required in a hotel investigation and restitution, which is our main objective.

Cooperation

When the police interview a suspect, they have to advise him or her of certain constitutional rights. We sometimes have to remind ourselves that we are not the police and do not have to do that. Our interviews are with employees and their participation is a condition of their employment. You should have a policy to this effect in your company policy manual, and you should remind employees of this when talking to them. Of course, they are free to leave at any time, but doing so will be cause for termination. It is advisable to tell them that before beginning an interview. This is a good time to remind them that lying or refusing to cooperate also may be cause for termination.

Having provided these admonishments, make sure the interview scene is nonthreatening. Do not back your subject into a corner where he feels he cannot leave. This could come back to you as false imprisonment or unlawful detention. There is nothing wrong with offering water, tissues, and restroom breaks. The old tales of the wobbly chair, bright lights, and threats of violence are reserved for the movies.

Unions

If your company has any employees in bargaining units, chances are they have wording in their contract allowing a shop steward to be present during interviews. A rule derived from The Weingarten Act provides any employee who is questioned by any member of management, where the questioning might lead to disciplinary action or termination, to have an employee witness present. The details of this agreement depend on the specific contracts in place at your property, so you should consult your HR Department. Failure to provide the shop steward during your interview may invalidate the information received and cause a union grievance to be filed, or worse—an unfair labor complaint. Once you establish this procedure with HR, make sure you follow it the same way each time you interview a union employee. In most contracts, the steward is not allowed to give advice or even talk, so it is not a big deal. In fact, you may be able to select the steward.

Translators

We mentioned earlier, regarding statements, that the translator you use should be one of your choosing who has training. What I have seen in most instances is the translator plays lawyer and speaks on behalf of one party instead of just translating. You can imagine how this can botch an interview where you are trying to reveal lies in the wording or certain statements that make the employee nervous. Even with a good, trained translator, it will be very difficult to do a good interview or interrogation. In a perfect world, you would have a bilingual trained investigator.

Burden of Proof

In a personnel investigation, we are not proving a crime, only a policy violation. We do not have the same burden (beyond a reasonable doubt) that has to be proved in a criminal setting. This is why we go for violations of policy rather than breaking of laws. For example, if you are investigating a theft (loss) from a storeroom, you only need to know that your suspect was in an unauthorized area, did not follow requisition procedures, etc. If you had to prove the actual theft, you would need a video camera or a witness who saw the suspect put the item in his pants. Suppose a guest complained that an employee shoved him. This may be a criminal battery. To prove that the battery occurred, you would need a witness, video, or something more definite. Unsuccessfully prosecuting an employee for battery does nothing for the hotel (or anyone else), but we can easily prove that he violated a guest service policy, was out of his work area without permission, had inappropriate contact with a guest, or any number of policy violations.

Because policy violations are not misdemeanors, they do not have to occur in our presence to terminate the employee. Since our property is not a court of law, we do not have to prove beyond a reasonable doubt that he did it.

> In O.J. Simpson's murder trial, the prosecution was not successful in proving beyond a reasonable doubt that he committed the crimes, so he was acquitted. In the subsequent civil trial, he was found to be responsible for the murders. Civil trials have a different burden of proof called "preponderance of evidence." This is substantially less proof required, and is therefore easier to prove. For the sake of this illustration, suppose Simpson was our employee and we wanted to terminate him because his involvement in the alleged murders was damaging our reputation. We would have many policy violations, not even related to the murder, that we would use to successfully terminate him.

Criminal Investigation

During an interview of what you suspected was a personnel investigation, the case may turn into a criminal investigation. For example, what you thought was a sexual harassment allegation might turn out to be an alleged battery or even sexual assault. Naturally, you would notify law enforcement as soon as you find out. The danger in continuing a

suspect interview may cross a line of acting as an agent of the police. All kinds of legal ramifications come into question, including should you now "Mirandize" the suspect; is the information you receive now protected by the Fourth Amendment; and is the suspect still free to leave. Better safe than sorry—inform the suspect you are calling the police and turn over everything you have to them. If you have enough to arrest the suspect to keep him from leaving, do so. The investigation now becomes a police matter and your HR Department can make a decision based on their outcome.

Keep in mind that your investigation may have to continue—without the suspect—to cover any civil liability. Even though law enforcement action may seem to take this to a certain level and out of your hands, the company may still be liable for a hostile work environment or something else depending on the original allegation. So, you will want to stay in touch with the detective or prosecution as it relates to company liability.

In order to stay in contact with the investigating agency, you should develop a supporting role. This means supplying video, handing over statements you already have, and seeking witnesses and evidence. Be sure to consult your counsel on what level you will cooperate with police. There may be proprietary information that must remain private and is subject to subpoena. Finally, make sure to keep copies of everything you give the outside investigators. If their case falls through or even if it does not, you may have to run a continuing, or parallel, investigation of your own.

Private versus Public

Many people in both private and public sectors have trouble distinguishing the difference between private and police investigations. The objective of a police investigation is to prove that the suspect committed a crime. Even if the investigation objective is to find a suspect, it is done knowing that a crime occurred. While there may be crimes occurring at your property that require investigations, keep reminding yourself that you are not the hotel police department. Your objective—your only objective—is to protect the assets of the company. After a loss has occurred, the only way to protect assets is to recover the loss and to prevent future losses from occurring. This is a novel way of thinking for some of us who have been engrained to solve crimes and catch bad guys.

If a guest suffers a loss, it is the investigator's job to either prove that it was not the fault of the hotel or recover the loss. For example, if a guest is missing his or her laptop from the room, and we can prove that no employee took it, and there was no responsibility for the loss, such as a faulty lock or no security, then the hotel has no exposure.

Restitution

We have talked throughout this and other chapters about recovering losses. This is commonly done through restitution. Restitution can be a valuable interrogation tool and a metric for showing security's contribution to the bottom line. It is generally a negotiated amount up to or equal to the amount of the loss. It can also include administrative, labor, investigative, and other costs associated with the loss.

During an interview, a common tactic is to use restitution as a bargaining tool. An employee who thinks he is facing criminal prosecution may be very willing to pay back

what was stolen or damaged. The investigator can negotiate on the amount and even payment terms in return for other information provided. Remember, this is a private agreement and has nothing to do with the crime or the police. That also means it will be harder to collect. You should try to get the majority of the amount out of the employee's final check because it is not likely you will see him again.

Court-ordered restitution is also a very viable source of recovery for the Security Department. An employee who is being charged with embezzlement or a "guest" who is being charged with theft can be responsible for restitution. This will depend on the initiative of the police officer making the arrest report, the detective who prepares it for prosecution, and the prosecutor. If all of them work with information you provide, the judge is likely to order restitution if the suspect is found guilty. Your department should have restitution letters that are filled in when an arrest is made. Include the loss amount and any associated costs with the arrest. Don't forget the labor costs of the arrest, the administrative costs of processing the report, and any other department costs. It is best to have these costs itemized in a list in advance, so the arresting officer can put these into a letter to go with the police.

Workers' Compensation Investigation

Security is not always the department dubbed to do employee accident investigations. I believe it is only natural for Security to use its trained investigators for this, especially because it may reveal employee misconduct. The Workers' Compensation Department, HR, or the insurance company usually initiates these investigations. If the explanation of the accident appears doubtful, if there are some suspected safety or policy violations, or if the employee is suspected of insurance fraud by making a false claim, an investigation is likely to be requested.

The process is very similar to the one for personnel investigations discussed earlier in this chapter. There may be different forms and report formats and the burden of proof may also vary, but the fundamentals are the same. As we proved a particular policy violation in the personnel investigation, for accidents we focus on four main conclusions:

1. Is it work-related?
2. Are there any safety violations or recommendations for future safety policies?
3. Was it caused by the employee, the company, or a third party?
4. Was there negligence on the part of the employee?

Each of these can cause a claim to be denied, partially paid, or deferred to another party. The insurance company will generally direct you to its main concerns. Regardless of what the insurance company decides, you may be directed by HR to find policy or safety violations that they will address.

Guest Claims

The fourth type of investigation involves guest claims. These claims (whether there is an actual claim or not) include guest accidents, loss or damage of guest property, food-related illnesses, and company-wide complaints.

Guest accidents are, by far, the most costly claim your property will handle. A slip and fall that involves back surgery or long-term loss of a bodily function or limb can cost hundreds of thousands of dollars. If the case goes to a jury, your little investigation might save or cost the company millions. This is not an exaggeration as the examples throughout this book have illustrated. Liability, safety, and prevention of accidents are addressed elsewhere in this book, so we will focus only on the investigation here.

Triggers

Your department may not have the work force or the time to investigate every guest report that comes through. If that is the case, you need to develop triggers that automatically start an investigation. For reports involving guests, here are some examples of criteria that would trigger an investigation.

Loss or damage greater than $250
Any guest injury
Complaints that are serious, such as discrimination
Where the return is greater than the cost of the investigation (sometimes it is cheaper to pay)

Statements

We discussed gathering statements in the section entitled Preliminary Investigation. The investigator will put that statement to good use because it is unlikely that there will be an interview or further contact with the guest. The investigator can use the information in the statement and see where it differs from the verbal account given to the officer. For example, when the watch was first missing, it was worth $100. When the guest wrote the statement later, it was valued at $500. When the guest calls your claims representative, it is now worth $5,000. We use the statement as we did with interviews, but in lieu of getting to speak to the guest.

Witnesses

Witnesses are handled differently depending on whether they are guests or employees. Employee witnesses are treated as they are in a personnel investigation: Obtain and evaluate statement and interview as necessary to gain more information. Guest witnesses can be contacted after they leave, but it is not likely to be in person if they are tourists. Phone interviews do not work well for discerning the truth, but are perfectly acceptable for following up to clarify what the guests wrote in their statements.

"Suspect" employees should be investigated exactly as with a personnel investigation. Remember that with a personnel investigation, the objective is to prove a policy violation. In a guest loss, we are trying to prove that we have no responsibility for the loss. These two objectives seem to conflict because if we prove an employee was responsible, then the hotel is vicariously liable for the loss as well.

Your Risk Manager or Claims Department may not want to investigate certain incidents because they can more easily deny the claim and responsibility if there is no evidence of hotel responsibility. In the old days, Security departments would keep their investigations confidential for that very reason. That way the claims person could pick and choose the investigative reports that favored the hotel. We all know this is wrong and no longer even true. Any documentation can be called into court, if it goes that far.

ANALYSIS

As I said at the beginning of the Investigations section, investigators are the most skilled employees you have. They can and should be used for other important functions than just loss recovery.

Metrics

"Metrics" means "to measure," which is why it applies to the socket set in your toolbox as well as the measurements of your department. In fact, toolbox is a good allusion for how Security uses metrics.

Measurements of the department come from a wide variety of data sources and are used for just as many reasons. One metric you are already using is your daily labor report. This report, from the company's timekeeper, tells you how much you spent on labor, how much overtime, how many hours, and so forth. The time clock is the data source, and the report is the metric. Someone put that metric together for the managers in your company based on what metrics he or she was told you needed. You could expand that report to include other measurements if you knew how to access the data and how to create the report. You probably do not "own" time clock data, but you do own other Security data, so all we need to work on metrics is a data source and a reporting tool.

Data Sources

Let's determine the types of data sources, then what metrics we want, then how to get from A to B. However, even if we do not know what metrics we need, the sooner you start collecting data, the more data you will have to work with when you are ready.

Most reporting systems (discussed in Chapter 9) create their own database and even have their own metrics. Some limit your reports to the metrics they created, but others give you access to the raw data and allow you to download it into a spreadsheet or reporting software. This is great, but you may still have to create some data for yourself. For example, not all car burglaries in your parking lot are reported to Security. Some people know that you are not going to reimburse them for a loss, so they make a police report and go through their insurance. In that case, you may download the raw data from your reporting software, which will give you dates, times, locations, value, etc. and then manually add the information you get from the police department. (Remember, we did this as part of our Risk Assessment in Chapter 1.)

If you do not have reporting software—by that I mean you do reports in a word processor or by hand—you need to create your own data source. This is not so difficult if done on a daily or weekly basis, which is why I mentioned starting now so you do not have to go back and do it when you decide you need to know everything that happened this year. Decide how you are going to work with this data. Excel® allows you to work with other reporting systems, so I would suggest Excel or similar spreadsheet software. Handwriting a table or spreadsheet will not allow you to format it for use in Excel, so avoid this wasted step if you can.

Creating a Spreadsheet

The secret to getting the most out of your data is to separate data into as many different categories as possible. In a spreadsheet, these data are the columns, such as date, time, location, names, etc. You could have 20, 30, even 50 columns if you include victims' names, witnesses, addresses, employee numbers, etc. In database lingo, this huge spreadsheet is called a flat table or database. A relational database is one that divides data into different tables and links them together by common fields. That is just some background information to understand the process. If you are going to do this manually, stick with the flat spreadsheet.

With manual entry, the hardest part will be setting up the spreadsheet columns with everything you want. As mentioned previously, get each column down to the smallest detail. Do not combine date and time or first and last name in the same column. It will be easier to sort and work with those columns if they have just one value. Once the blank spreadsheet or database is created, someone needs to enter the data daily or weekly. This should only take a few minutes as the person doing it starts in row one and enters the information horizontally for each report or incident.

A spreadsheet like Excel allows you to do most things like sorting and adding, but a more advanced system like Access or Crystal lets you combine data sources called "tables," create formulas for working with the data called "queries," and format it into a presentable report. You can get most anything from your raw data with these programs. As we get into crime analysis, we may want to know which housekeeper is common to the most room losses, what times of day most of our vehicle burglaries occur, or if the number of patrol routes has any effect on slip and falls.

Crime Analysis

It is the responsibility of the Security Director to be preventative more than reactive. Even police departments that traditionally focused on reacting to crimes and trying to catch criminals on the back end are now using crime prevention techniques to reduce the chances of a crime occurring in the first place. We already know physical prevention techniques and they are discussed throughout this book, such as layered security, preventative patrol, and behavioral analysis. Another important method that you should be using, and may already be using to some extent, is crime prevention analysis.

The concept is to use data, as we did in our Risk Assessment, to prevent crime by investigating patterns. As you analyze crime statistics, you will notice trends that suggest certain commonalities. Burglaries may occur on certain hotel floors, at certain times of the day, or

by certain methods. Crime (or incident) analysis is the sorting of data to reveal patterns, exceptions, and trends. Now that we have a spreadsheet with some data, or a reporting system that provides us with presorted information, we can start to see what we have. There are many ways to look at the data and you really need to look at all of it for it to be of any use.

Location

You may start by dividing your property into general locations, such as garage, guest rooms, nightclub, and lobby. These areas are so different that there probably will not be any overlap of crime or incidents. In other words, statistics that you derive from the garage or parking area will not likely be related in any way to crime you have in guest rooms.

Once you separate these areas, you can work on data from each one separately. In each of these areas, you will want to have sublocations, or locations that are more specific. These may be floors in a garage, or quadrants in a parking lot. In the hotel, it would likely be floors. In the public areas, you have the lobby, each restaurant, bar, etc.

When you sort by these areas, you may already see patterns, such as one particular floor that has problems over another. In Valet, or the nightclub, of course, every incident is in that location, so skip this step for those specific areas. If you notice a trend or something unusual about a particular location, there must be a reason and that is what we are here to solve.

Crime Type

The next "sorting" method of analyzing crime data is by type of crime. This will show you at a glance if you have more of a problem with damaged cars in Valet, rather than property loss; or property loss in guest rooms, rather than assaults or robberies; or more fights in the nightclub than missing purses.

Time

The next sort option is date and time. Here you are looking for commonalities related to time of day, day of week, shift, etc. Perhaps most car burglaries occur between 7 p.m. and midnight. Maybe room losses usually happen during the day. Fights in the nightclub occur most often on Wednesdays. (This seems very elementary to most of you, but you need to follow the steps to ensure that you do not overlook anything. We will get further into the analysis shortly.)

Suspect

Another sorting option of our crime data is the suspect. The obvious pattern might be a housekeeper who has coincidentally cleaned all the rooms where losses occurred. Less obvious are profiles of suspects. You probably do not have suspects identified in most cases. However, in nightclub fights you should have descriptions. Do white males in their early twenties start all the fights? The same goes for losses in the kitchen. You can rule out a bunch of staff members if the suspects all had grey shirts and the kitchen staff has white shirts.

Other Sorts

If you find commonalities in your data, it will be worth it to drill down deeper into other categories. These may include specific room numbers, approximate times, etc.

Crime Triangle

Three of the categories we just talked about make up the crime triangle. This triangle is a useful illustrative way to solve and prevent crime.

The crime triangle consists of three components of a crime: location, victim, and suspect. Every crime must have a victim, one who suffers from the crime; a suspect, one who commits the crime; and a location where the crime occurred. (The location may be virtual, such as the Internet or telephone.) Take away any of the three components and there is no crime.

Suspect

The suspect leg of this triangle is traditionally the one we go for. The suspect is the bad guy, the one breaking the law, so that is generally where we concentrate our efforts of solving crimes. If a neighborhood is having a rash of car burglaries, the police try to catch the bad guy and, thus, eliminate future crimes. Of course, this is great if you can do it, but it is best to let the police do that and for us to concentrate our efforts on preventing the crime from occurring again. Catching the suspect may prevent the suspect from committing the crime again, but it is only one third of the prevention. Someone else can come along and commit the same crime, theoretically.

Without getting too far into psychology of a criminal, it is important to understand a little bit about his/her thought process. When most of us make a decision between good and bad, we use rational judgment that takes all of the factors into account: How will this affect the other person? Will I be caught? What will happen if I am caught? How would I explain that to my loved ones? And so forth. Most of us choose not to commit the crime because of the way we answered those questions. (This may explain why alcohol turns normal people into criminals.)

The criminal mind generally works a bit differently. The thief or assailant does not ask himself those questions (until afterward, maybe). He sees the immediate gratification of possessing the item, committing the violent act, or the thrill of the bad act. This makes most criminals opportunists and shortsighted thinkers. It helps us to know this because we know that if we decrease the opportunity or make it more difficult or time-consuming to commit the crime, we can prevent many of these acts.

For example, a wallet lying on a counter unattended is too tempting for someone who does not ask himself the questions. He sees an opportunity and takes it. If the owner is standing near the wallet, it becomes less of an opportunity and less tempting because the immediate gratification becomes less likely because the person may fight him. If the owner is holding her wallet, that makes it far less tempting. The gratification is now out of sight to most (unless they are a skilled snatcher and do not see the person holding it as a deterrent).

One exception to this theory is the criminal who "justifies" his actions. It should have been mine anyway; they don't deserve to have it; they can afford to lose it; she hurt me so I will hurt her; he fired me so I will show him who is boss; etc. Since we know there are criminal minds out there, and plenty of justifications, we have to limit the opportunities.

Victim

Of course, if we get rid of all the victims, we can certainly prevent crime. That is not very conducive to the hospitality business. Seriously, we can have some influence on potential victims to prevent them from becoming victims. We do this all the time by warning vehicle owners to lock their cars and not to leave valuables inside, providing awareness training, posting signs warning patrons, etc.

Anything you can do to get hotel guests out of the "tourist/victim" mentality and make them more self-aware is a way to prevent crime. We want our guests to have a worry-free stay in our establishment so we have to find a reasonable balance between paradise and prison.

Location

Naturally, if you change or eliminate a location of a crime, it will not happen again—at least not there. This is also a common prevention technique we use. If crimes are happening in a certain area, we beef up or patrol, install cameras and locks, etc. Consider these measures in your hotel.

The crime triangle is something you were already using, and maybe did not realize it. However, when you approach crime prevention using the triangle model, you will focus on all three legs, rather than just one. This gives you three times the opportunity to prevent the crime. As you review crime trends from the data you compiled, determine which leg provides the commonality. Location is easy. More car burglaries are occurring on the fifth floor of the garage or door pushers keep hitting the same room, which has a faulty closure. These are easy crime trends to address.

Sometimes the trend is not location, but suspect. For example, if you have a problem with graffiti, it may happen all over the property, but you can develop a profile of the suspect easily. It may be video, or you may know what gang the suspect comes from. Then your prevention step might be to identify those persons and watch them or exclude them.

Finally, the data may show that the commonality is the victim. The obvious example would be little old ladies who keep getting robbed of their purses. You may want to put more resources on watching little old ladies with purses, warning people not to carry cash in their purse, or providing awareness training.

Off-Property Incidents

In Chapter 1, we mentioned the importance of gathering outside data for performing the Risk Assessment. Investigators or analysts are usually the likely persons to track this activity. Besides assessing risk, we need to know what is happening at other hotels (or similar properties) and at neighboring businesses and streets. The criminal activity in our neighborhood has many affects on us. It makes or breaks our reputation, makes our guests and employees feel threatened, and determines what types of security measures we will take.

Street crime near your property may prompt you to install lighting, locked gates, fenced parking, etc. Other hotels with a propensity for crime may encourage you to take preventative steps to avoid those crimes on your property. Gang activity in your neighborhood will decide whether you have dress codes, controlled entry, or even armed security.

For all of these reasons, track activity on a spreadsheet just as you do for internal incidents. List the major incidents specifically, such as with a news clipping, and other incidents by category and location. If applicable, list the security measures you took to reduce the chance of those crimes happening.

Reacting to the Data

Measuring the incidents we have, sorting the data, and analyzing it not only provide nice reports for the boss, but also can help solve the problems, thereby protecting the assets even better. The traditional method was to go after the bad guy. But, the crime triangle shows us that the bad guy is only a third of the problem and not necessarily the easiest side of the triangle to remove. Remember that our job is to protect the assets. The most efficient way to do that is through prevention. Arresting people, or even firing people, does not always prevent the loss.

So, what else can our crime analysts recommend to prevent future crimes or losses? The answer is in the data. Look at the information you have and determine the most efficient method of preventing it from happening again. Lighting, cameras, locks, patrol, training, awareness, and special operations are just a few of the tools at our disposal, and the solution should be obvious in the crime data.

SPECIAL OPERATIONS

After performing a crime analysis or beginning a specific investigation, it may be determined that the suspect leg of the triangle is the one we need to remove. As long as we admit that this will not be preventative in nature and will likely cost more, it is perfectly justifiable to go after the suspect, especially if it is an employee. These temporary operations are designed specifically to target one suspect or a group of suspects. Operations include undercover officers, outside agencies, or covert cameras. They may include targeted area patrols, new procedures, or training.

Undercover Operations

Undercover operations encompass a wide variety of plainclothes, covert, or discreet investigations depending on the objective. I find that either Security Departments do not use them enough or they use them too much. The advantage of a discreet operation is that it addresses those offenders who are privy to the visible security measures. Disadvantages are that they are not very preventative in nature—more reactionary—and often take resources away from other necessary areas.

Outside Agencies

It may be appropriate at times to ask local law enforcement agencies to conduct a special operation on your property. Naturally, this method can only be used for suspected criminal activity. If your problem is a policy violation or anything less than criminal, the police

cannot be of much help. However, they may be very interested in working a known problem with prostitution, drug dealing, or fraud.

If police detectives are assigned to work your property, you will be placed in a supportive role. You should provide whatever information they need and whatever technical support you can. See the section on Prostitution in this chapter. Suggestions for law enforcement investigations include prostitution, organized crime, drug sales, car burglaries, etc.

Private Outside Agencies

Other loss investigations should not be handled internally. A complicated internal fraud case is an example of an investigation that requires a great deal of resources, an unknown undercover employee, and a perspective that is strictly unbiased. Even if you are confident in the ability of your staff to perform this operation, and to do so without favor, remember that perception is reality. The outcome may be questioned morally or even legally if there is even a hint that your relationship with co-workers affected the investigation.

There are many very qualified private investigators to use for such an investigation. If you do not know someone who can give you a personal recommendation, go through your local security association or police liaison. Your company law firm may have a reliable company that they have used in the past. This is not a job to be chosen from the yellow pages.

Like the police, you will have to hand the entire matter over to this outside person. As with any secret, the more people you tell, the less likely it will be a secret. Every executive wants to know and thinks he has a reason to know, but it is better if only one person knows.

Use the guidelines set out in the Personnel Investigations section of this chapter in defining your objective, what the expected outcome will be, if there will be charges filed, a term, etc. Suggested uses for an outside employee investigation include fraud in the Accounting Department, bartenders stealing, Receiving Department losses, nightclub doorpersons stealing, employee drug use, etc.

In-House Operations

It is almost impossible to have your investigators operate undercover if targeting an employee. Use an outside company if your investigation is internal and requires undercover personnel. Some internal investigations can be done with video. This process is generally like fishing. You place some bait, get the right equipment in place, and wait for someone to come along and bite.

One common place we do this in hotels is guest rooms. This is a huge waste of time unless you have narrowed down a suspect to a housekeeper. Let's do some math.

Suppose you have an average of 500 hotel rooms occupied every night. And suppose you average one room loss per day (night). Further, suppose you have time to set up a room two days per month with an investigator, video camera, and bait. That is a 1 in 7,500 chance that you will be at the right room on the right floor where the right housekeeper is tempted by the right bait. Unless you narrow down those odds, you are throwing away resources. Recall our crime analysis previously in this chapter. First, make sure it is a housekeeper. It

could be a door pusher or a cohabitant of the room. Second, see if any housekeeper is common on more than one room loss. Third, narrow down the bait by determining if there are commonalities with the property taken (cash, jewelry, etc.).

If you have a suspect employee, a probable day of the week, a preferred floor, and type of bait, then you have a better than 1 in 10 chance. That is worth it, but still not guaranteed to catch anyone.

How to conduct this operation is the easy and fun part. You will come up with some neat cameras and other equipment to do this because your motivation will be there. I just want to make sure you put the proper preparation into selecting the location, victim, and suspect to target before you begin.

Covert Cameras

Covert cameras are those that are hidden from view or disguised as something else. Before you even think about using hidden cameras, check with your legal counsel on issues such as expectation of privacy and wire-tapping laws. There is no specific law about where to put cameras. The precedents are set in federal and state case law about what is reasonable. We also follow different rules than the police do because we are private. There are now very specific laws in each state about audio recording. These laws come from older wire-tapping laws. Some states are keeping up with technology (to include video) and others are not. So your state might forbid recording an audio conversation and allow (by lack of any laws against it) video recording.

A New York jury awarded a man $3 million after he sued his employer for discrimination. The man had made several complaints regarding ethnic slurs from his co-workers. There was no apparent investigation of the slurs, but a camera was placed in the man's work area to watch him, presumably to retaliate for his complaints.

Cameras are a good way to document misconduct or criminal activity, but should never be used in this manner. The Security Director or Human Resources Director should authorize such use of cameras to ensure that employees are investigated fairly and that labor laws are not violated.

To keep you out of trouble, here are some rules that should cover you in most states. Do not place a video camera in a place where someone would expect to have privacy. This includes bathrooms and dressing rooms, but also may include a private office or even a storeroom. Make sure you have a documentable reason why you need a hidden camera there. Reasons include a rash of thefts from the area, reports of misconduct, such as sexual activity or sleeping, and suspicion of fraud on a computer. Do not place a hidden camera in an occupied guest room. Consider a general policy about video surveillance for all employees. Do not audio record someone in secret.

Some great ideas for camera placement have been used in hotels by clever investigators. Your networking with other directors and investigators will give you good ideas and save you from duplicating mistakes.

Room Losses

Set up two rooms—one with bait and camera, the other with video equipment and investigator. Use bait as discussed previously, depending on the potential for loss, and check the integrity of everyone that comes into that room. This will include the housekeeper, bell person if you make a reason for them to be there, engineer if you call in some maintenance request, and security for lost and found. After you have tested those with access, try leaving the door ajar. This will attract what are called "door pushers" (opportunistic thieves who look for open doors in hotels). You can arrest them if they steal something or 86 them if you prefer. This will test security and other employees as well to see if they take action when they spot an open door.

There is much folklore surrounding the origins of the term "86." We know 86 as the popular term for trespassing someone from our establishment. Nevada hotels are the most notorious for this service, which occurs many times every day in casinos and bars throughout the state.

One origin of this term comes from the Old West days. When a bar patron was becoming too drunk or creating a disturbance, they would serve him alcohol that was 86 percent (172 proof). That would pretty much knock him out. I doubt that is your policy now. Other explanations for the term come from addresses of famous bars on the East Coast, section numbers of liquor laws, and a cross-out method used for taking items off menus. The F-86 Sabre aircraft had many notable "kills" and other successes throughout history.

There are numerous camera options available these days due to their smaller size. Cameras can be secreted in almost anything and if you have a technician available with a little imagination, she can probably put a camera in just about anything.

Suggested uses for in-house operations include losses from guest rooms, storerooms, valet vehicles, and lockers; employee vandalism; safety violations; and harassment.

Bag Checks

The ideal policy would be to have a security officer inspecting every employee who leaves the employee areas (back of the house). This is often considered not worth the labor required, or not practical due to the layout of the basement or employee area. Twenty-four-hour inspection posts are certainly expensive, so it may be worth it to do random bag checks.

The unfortunate fact is employees walk off your property with company merchandise every day. Whether it is shampoo, towels, and soap, or alarm clocks and hair dryers, or even alcohol and guest property—chances are there are some thieves among us. A simple deterrent to this is to do bag checks daily at the end of shift or at least randomly.

Bag checks are simple and can take less than 30 minutes. Station two officers at the employee exit and inspect every purse, backpack, and duffle bag that comes through. Do not target housekeepers. Require every employee to go through this process to be fair.

Make sure the second officer is watching for employees who see the inspection site and head back to their lockers.

A hotel had an employee inspection post that ran 24/7 for many years. During hard financial times, that post was closed. A few months later, the director of Security decided to institute random inspections. On the first day, the very first employee who walked past the inspection area was a housekeeper with an alarm clock in her purse. Several more were seen turning around and heading back to their work area.

Investigators can assist with bag checks and take the opportunity to specifically watch certain employees who appear in their metrics more than others do. They also may want to set up an integrity check of storage areas and use the bag check to check for stolen products.

Make sure your company has a policy about employees being subject to search. Signage is a good reminder.

DRUG TESTING

According to a study performed by George Washington University, the hospitality industry employs the largest number of workers with alcohol problems. Alcohol is just one part of a nationwide drug problem that is woven into the fabric of our workforce. Whatever the statistics on substance use or your own personal feelings, we can probably all agree that it has no place at work. Besides, if the company has a policy against it, it is your job to enforce it.

Companies generally do drug testing in four different circumstances: pre-employment, postaccident, random, and cause. I will assume that you have little to do with the pre-employment screening, so we will discuss the other three, which are almost identical processes. First, a brief discussion about drugs.

For our purposes, we can classify mind-influencing or psychoactive drugs as either stimulants or depressants. (This is over-simplified for illustration only.) These "controlled substances" are alcohol, marijuana, prescription drugs, and street drugs. Each of these substances affects judgment and physical skills and, therefore, can cause accidents and poor work performance and place a company in a bad light.

Most drugs take effect on the mind and body within about 30 minutes. Their effects can last up to four hours in most cases. (That means someone who is under the influence in the second half of his or her shift most likely consumed the drug while working.) Testing methods include urine, blood, and saliva. (Hair testing does not work to see immediate effects so it is used for pre-employment screening. Sweat, or patch, testing is used to check for usage over a long period.)

Your HR professionals, legal counsel, and company medical provider should decide testing methods and policies. Some bargaining agreements have special stipulations about testing methods that must be followed. Whatever your procedures are, these are my recommendations and you can adapt them to meet your requirements.

Random Testing

Most companies do not allow for random testing (except for regulated employees like bus drivers, airline pilots, and sports figures). The accusations of discrimination and favoritism

are too difficult to defend for normal workers and it is difficult to administer. If you do have random testing, it is likely that Security will not be involved, but if you are, follow the procedures in the next section.

Postaccident

Almost every company requires a drug test following an employee accident. Your company will have to decide if this is done for every reported accident, those that just claim injuries, or those that require medical treatment. I would suggest any accident where an injury is claimed gets a drug test. Before any testing is done, the employee should be required to sign a policy statement with a witness. The policy should state three things:

1. The company requires the test and refusal to take it will result in termination.
2. If the test comes back positive or has to be sent for further testing, the employee will be on investigative suspension.
3. If the test is positive or requires further testing, the employee will not be permitted to drive home.

To save time and money, I recommend using a swab test that can be given by Security. These tests are a few of dollars per use, test for a wide variety of drugs, and give immediate results. If this test is negative, it is finished. If the swab were positive, I would have it corroborated by a professional lab. This will avoid a $10 test that was administered by an untrained security officer being challenged later. Swab tests also do not have thresholds, which means someone on a legal, prescription dose of valium would come back as positive.

They make swab tests for alcohol or you can use a breathalyzer, which provides a blood/alcohol percentage. This may be important to your HR Department because it is written into most labor agreements.

Lab or clinic testing should be of the type recommended by your medical provider. They may want to do urine, blood, or both. Urine testing means the employee has to pee in a cup. The clinic will tell you all sorts of stories about how these are defeated by guilty employees, but the clinic personnel know how to spot deceptive tricks. The blood method involves drawing a blood sample. Different substances stay in the urine and in the blood for various durations and at varying levels. The comparison of blood and urine helps the lab technician decide the level of effect that the employee has. If you have a local medical clinic that is available 24 hours, you will have to have someone drive the employee to the clinic for testing. Most clinics will provide preliminary results immediately. If there is a suspected positive, they will send the sample to a lab and results may take one to three days.

If prescription drugs are indicated in a test, the lab will usually contact the employee to justify these medications and provide prescriptions. The level in the body must meet the amount prescribed. Most lawyers will not allow a termination for prescription drug use.

Cause Testing

Testing an employee for "reasonable cause" is quite a bit more subjective than postaccident. The justification is not as clear, but with the right policies, we can make it simple. You should start with a policy that allows for drug testing if there is reasonable suspicion that

an employee is under the influence. Then require a manager to have that reasonable suspicion. No special training is involved if you use the "reasonable person" test. Assuming your managers are reasonable, they know what behavior is unusual or possibly related to substance abuse. To avoid accusations of targeting, require the department manager or supervisor to get a second opinion from the Security Supervisor. The two supervisors should be able to agree that they smell alcohol, note strange behavior, hear slurred speech, and see dilated or constricted pupils or a staggering walk.

The testing procedure after that point is the same as for postaccident. Fortunately, the swab testing is noninvasive and does not take the employee off the job very long if it is negative.

PROSTITUTION

As mentioned throughout this publication, prostitution is a big problem for hotels. When I was a young Security Manager, my very experienced hotel manager told me, "Prostitutes are good for the hotel business." He was obviously referring to keeping guests happy and bringing in new business. Unfortunately, the sex industry is not glamorous, far from it, and the criminal negatives far outweigh any business positives. These next few sections on prostitution are my opinion, but they are based on factual experience.

If you have no experience with the criminal side of prostitution, forget about the movies and the stories that glamorize it. Prostitutes are not working their way through college, they are not aspiring actresses, and they are not engaging in a victimless crime. They may have started that way or may have even been lured to this way of life with those promises, but 99 percent of them are motivated by drugs. If the pimp (or "daddy") does not bring them into the business, he will take over their business by force. Drugs are used as a reward and create a dependent relationship with the male. The male pimp uses violence to force a submissive relationship where the female is rewarded by pleasuring him. This reprogramming turns the prostitute into a drone seeking money for sex, which earns favor with the pimp, which earns her more drugs and membership in the pimp's "family" or "stable." The pimp, who is grooming his own interns of his trade, sends young men to be the escorts of the prostitutes. As you can imagine, this dysfunctional network has huge potential for violent crime. Here are some examples seen in hotels.

The pimp ("chulo" in Spanish) will rent a room for the prostitute to work her business. She will work the hotel bar, club, or even the street and bring men back to her room for the transaction. Often, this deal goes off without a problem. Occasionally, the protector, who gets greedy, will "roll" (rob) the client ("John" or "date") in the room, taking his money by force before or after the sex. A certain percentage of the sex deal has to go back to the pimp, so the intern is motivated to make some money on the side. The room also can be used along with the Internet to be a home base for callouts. Callouts are appointments made by phone or Internet where the prostitute is called to the client's hotel room.

A prostitute may be called to a guest's hotel room on a callout as described previously. In that case, the pimp or protector may accompany the female and wait in the hall or even the lobby or bar until the deal is complete. A harmful version of this is when the prostitute leaves the door ajar for her male friends—or just lets them in—and they come in and rob

the victim. This is often a very violent robbery because the pimps need to show their hookers and others that they should not be messed with. These "guerrilla" pimps rely on the fact that most victims would not dare report this crime.

The classic and most common prostitute crime is where the prostitute goes into the wallet of her victim while he sleeps and leaves before he notices. This turns into an expensive lesson for the salesman from out-of-town who would not even dream of reporting he got ripped off by a prostitute.

Preventing and watching for these types of criminals involves a lot of experience and behavioral profiling.

Front Desk

Clerks at the front desk are experienced at this type of profiling and can spot a prostitute or a pimp immediately. Local IDs, young males or females traveling alone, provocative dress for the female and street clothes for the male, big handbags, but no luggage, and interest in Wi-Fi service are all possible indicators. Combine those indicators with the instinct of dealing with them regularly, and the Front Desk clerk can be a great resource. Have the clerks tell you when they check in suspicious guests so you can keep an eye on these folks and their activity.

Bell Desk

It is universally known that bell persons are the ones to go to for prostitutes. If they are not acting as a direct agent, they definitely see what is going on and can be a good resource. Enforce your policies and get them on your side in keeping trouble out of your hotel.

Suspicious Persons

Security officers should be alert for males loitering around hotel rooms, in the lobby, or at bars, especially if they came in with a woman and are now alone. Women who frequent bars alone, drinking very little, and especially leave with different men work inside hotels and are usually perceived as a bit classier than streetwalkers. Streetwalkers entering the hotel almost always carry a large shoulder bag where they keep cosmetics and a change of clothes to get ready for the next date.

Hotel Rooms

Housekeepers can usually tip you off to a room that is used for prostitution. Cosmetics without luggage and sex paraphernalia, combined with a laptop and drugs are positive signs. Of course, Housekeeping may notice the clientele coming in and out. Pimps and other members of the stable may use the room to sleep during the day after working all night. Housekeepers (and most employees) do not need awareness classes on prostitution. They know what it is and what it looks like. They do need to know it is a concern for you, so that they will tell you when they see it.

Homosexual Prostitution

Same-gender prostitution is just as prevalent but not necessarily as visible. There is usually not the same level of violence and drugs, but they are still present. Transvestites are sometimes called "dragons." Lesbian prostitutes ("jaspers") are very difficult to spot because they do not wear the flamboyant clothing associated with a heterosexual prostitute. Their behavior, like any other "freelancer," is obvious when working your bars or when accompanying clients or "marks." A pimp-less prostitute is called a "renegade."

Outside

I doubt you have streetwalkers working the corner in front of your hotel. Take a drive around your town, or just ask the police, until you find the nearest "track" (street where prostitutes await clients). Get a look at these persons so you can identify them when they come in your hotel.

Intervention

If you do find a prostitute, either known to you or from her behavior or a tip, never approach her with her client. This is extremely embarrassing for your guest. First, you may be wrong and then you end up accusing his daughter or girlfriend. Second, he will be embarrassed to the point of leaving your hotel and blaming it on you. She will not be embarrassed at all and will accuse you very loudly of profiling or discriminating. Third, he may defend her and embarrass you. I have been in all of these situations and will never repeat them.

Instead, approach the woman when she is alone. Simply trespass her from the property. Never give a reason, mainly because you cannot prove it. If you just want to interview her, that is fine too. This will let her know you are aware of her and will know who she is if anything happens. Talking to Johns is not recommended. It does absolutely nothing to protect the hotel and, as mentioned previously, just embarrasses all involved.

Many hotels that have a big problem with prostitutes working their floors and bars find it worth the time and expense to devote some effort to this problem. First, you should attempt to get your local authorities to run an "operation" in your hotel or at your bars or both. They may have a special unit that works these cases and can do the work for you. Most police departments understand the sensitive nature of these operations and will sincerely try not to disrupt your business or damage your reputation.

One method is for them to use two or three rooms that you provide. One is the bait room, another across the hall is within sight, or where surveillance equipment can be monitored. The third may be a holding room or processing room. The police may use certain Web sites where prostitutes advertise to lure them to the room. When the prostitute comes to the room, the deal is recorded, and then the arrest is made. The suspect is then taken to the holding room for processing and transporting off property. I suggest providing police access to service elevators and any other facilities to avoid mixing with guests. Police are generally sensitive to this and will cooperate in exchange for you making it convenient. You also can arrange to photograph and trespass the suspects. Remember that the prosecution does not matter to the hotel. The fact is that the suspect came to

your hotel on an invitation from a Web site and is not wanted there. Sometimes you can find the pimp nearby, whom the police cannot arrest, but you can trespass. Note: Do not cooperate with the police who want to target Johns. This does not benefit the hotel and is likely to snare a hotel guest or two. You want the word to get out to the prostitution community that they could run into a trap at your hotel, but not the salesmen from Iowa. That just hurts business.

Another operation the police can do is one that is a little easier for your staff to do as well. This involves a decoy at the bar to attract freelancers. For the police, they have to complete the elements of the crime, which include the arrangement of the transaction. As agents of the hotel, we need absolutely no reason at all. So, if someone comes up and says, "Looking to party?" then that is enough for you. Either way, especially if the police are involved, do not make an arrest or approach in public. This looks very bad. Accompany the suspect away from the bar and take care of the situation there. Once again, discourage the police from conducting operations that target Johns at your bars.

ABANDONED LUGGAGE

A Security Department could drive itself crazy if it overreacted to every suspicious bag. To avoid the anxiety and work force drain that these incidents can cause in a post 9/11 world, take these basic steps.

Risk Assessment

In your initial Risk Assessment, you should have determined your likelihood for a terrorist attack or bombing. A hotel in Islamabad has a much different expectation and reaction to an abandoned bag than one in Billings, Montana. In Israel, for example, every citizen notices suspicious packages and they are programmed to immediately clear the area and call the authorities. You will adjust your response accordingly, but the rest of this section outlines reasonable steps for most U.S. hotels.

Back Track

The more people you have watching for suspicious activity, the better. This was explained in Chapter 2. The sooner a suspicious item is found, the easier it is to find its owner or who left it, and what their intent is. First, make sure employees are watching for guests leaving their items unattended. Forgetfulness is very common for people on holiday, so reminding them not only protects them from theft, but also the hotel from a long ordeal. Second, check with employees or even guests in the area to see if anyone saw who left the item. Third, look for clues on the bag before touching it: nametag, plane tag, or any identifying marks. These can be checked through the Front Desk. Fourth, if necessary, look at video. If you have adequate camera coverage, you should be able to see who left it and whether it was an accident. If you do not have coverage of that area, you may at least have coverage of the person bringing it in the front door or out of the elevator.

Internal Procedures

We have learned from terrorist history that there is usually a dry run and surveillance before an actual incident. A dummy bag may be left and then the action taken may be observed. A bomber who is leaving a bag obviously wants to get far enough away to be protected and avoid capture or he would just detonate while he is holding it. Following this logic, it is best to have a quick, efficient procedure for dealing with unattended bags. Besides the identification process described previously, provide officers with a basic bomb awareness class. This will help them notice the obvious signs of a bomb such as smell, stained fabric, protruding wires, etc. Train security officers to remove the item immediately—after a cursory check—and take it to an isolated area.

Official Response

If your bag or package has made it this far in the process, you have a genuine ordeal on your hands. Your likely next step is to call the police. By the way, this should not be the first time you discuss this scenario with police. Find out in advance how they want these situations handled and what their response will be. It will likely be to send a patrol officer who will make his own assessment. He will call a supervisor who will make her assessment and call the fire department or bomb squad. I guarantee none of them wants to err on the side of being blown up, so they will always take it to the next level. By this time, the area will be evacuated for hundreds of yards and your business will be closed during the investigation.

Large hotels such as those in Las Vegas and New York that consider themselves likely terrorist targets find it is worth the extra expense to conduct their own investigation prior to calling law enforcement. Shutting down a hotel in Las Vegas for two hours not only causes hundreds of thousands of dollars, but it will make world headlines. By that time, bomb or not, you have a PR nightmare. The expense mentioned involves proprietary bomb dogs, electronic sniffers, and x-ray equipment. These are costly items, but when placed against the costs mentioned, they provide a good return on investment.

(See Chapter 10 for more on bomb threats.)

INTERNAL CRIME

It is said that while you are trying to prevent one thief from entering your front door, there are six leaving out the back door. That is not a statistic on doors, but on internal theft and fraud.

We prevent and detect internal crime a few ways. First is patrol, which is discussed in Chapter 8 and in this chapter. Regular, uniformed patrol helps prevent some general theft but rarely catches a thief in the act. Second is internal audit. Internal audit is generally an Accounting or other oversight body's function and not ours, but we will talk about it as an overview. Third is the Security audit. This is not to be confused with the special operations discussed earlier in this chapter. I will explain the difference shortly.

EMPLOYEE CRIME STATS

75 percent of employees steal once—50 percent of those steal again
20 percent of revenue is lost to employee theft
38 percent of shrinkage is employee theft
Workers spend an average of 7 hours per week goofing off
1 in 6 workers drink or use drugs at work
50 percent feel one gets ahead based on politics, not hard work
25 percent expect to compromise their beliefs to get ahead on the job
Only 20 percent are "very satisfied" with jobs

Internal Audit

Let's face it, a uniformed security officer (or even an undercover one) has no chance of detecting an accountant who is transferring money to his own account, or a department head who commits payroll fraud. This is done through checks and balances performed by the company. In fact, new accounting regulations enacted after Enron and other scandals now require outside oversight in most businesses. So, sometimes we see independent accounting firms going through the books. Frankly, these people are looking for major book juggling and are not likely to catch a kickback on a mattress.

However, accountants are on the same side as Security and we are all trying to protect the assets. Rather than work independently of them, we should work as partners. This is a relationship and a process you will need to develop through your general manager if you have not already done so. Your Auditing Department (accounting, compliance, whatever you call it) is auditing all day every day. This is a routine designed to catch and fix mistakes, prepare reports for the boss, and generate tax reports. These auditors may not be looking for fraud and might not even notice it unless someone tells them what to look for. In the payroll fraud example below, a fictitious employee is created and paid. An auditor is looking to see that hours on the check match the time clock, that the amount of the check is correct, and that the proper department was billed. If you ask them to look for duplicate addresses on checks, employees who always have the same hours, or checks that are always mailed (to name a few), they could alert you to these exceptions and you would do a follow-up audit. More on this later.

Security Audits

Security has the unique ability to watch employees. Observing an employee perform his job is the only way to prove he is stealing. Accounting or their boss may suspect theft, but the only way to catch it is to see it. An investigator performs an audit by watching an employee for a certain period and observing that procedures are followed and that the transactions are accurate. Procedures are developed to prevent loss. Examples of procedures are counting out change twice to a customer, closing a cash drawer between transactions, and checking ID on credit transactions.

When procedures are not followed, the employee will make a mistake, be taken as a victim, or commit a theft. Unfortunately, the chances of catching a thief in a one-hour audit are slim, but catching the procedure violations is common. Correcting the procedure violations will prevent mistakes, prevent robberies and thefts, and let the employee know he is being watched.

Establish a procedure with each department (not just cash handlers) so you can perform effective audits. You will need their procedure manual, schedules, and what they want audited. (You can audit smiles, uniform appearance, and time of transactions also). Once you have this information, set up a form or medium where you can get the audit information back to the department for follow-up. Of course, if you do catch a theft live on video, you will need a predetermined procedure for pulling the offending employee and conducting an investigation.

Types of Audits

Regulatory—These are not common in most hotels, but if you have departments that have to conform to certain governmental regulations, you will need to audit them to ensure they are following those regulations.

Performance—A performance audit is designed to evaluate employees doing their job. The topic may be guest service, number of guests served per hour, or duration of breaks.

Integrity—This audit is the type described previously to check for procedures that prevent loss.

Guest service—Most hotels have specific guest service policies, such as eye contact, smile and greet, providing directions, offering assistance, etc. Video audits are the best way of evaluating compliance with these policies.

Performing Audits

The first and best way to decide who gets audited is based on tips. Tips may come anonymously or they may come from a manager who suspects misconduct. They also may come from internal audit or some data where a strange pattern or exception has been identified. In the absence of any suspicions, the next way is to perform audits randomly. You may already decide that you will do one audit per week for each department. Then try to hit different employees on all shifts and in all areas. You cannot be truly random, but avoid picking on one department, gender, race, or union.

Most audits can be performed in about an hour unless there is a specific reason for going longer. If you are looking for specific types of transactions, frequency of breaks, or opening and closing procedures, you will need to adjust duration accordingly.

Next, we will review some common areas of theft and fraud that you can audit or at least be aware.

More internal (and external) theft can be prevented by strong controls and procedures rather than security investigations. There are two important components to a strong internal controls program. First is developing the proper controls. There are industry practices to follow for each job type. For example, cashiers are trained to follow several routine procedures, such as counting out change twice, checking counterfeit bills, and how money is

FRAUD DETECTION

Tips from employees (26 percent)
By accident (19 percent)
Internal audit (19 percent)
Internal controls (15 percent)
External audit (11 percent)
Tips from customer (9 percent)
Tips from vendor (5 percent)

These stats lead us to several solutions and one conclusion: Most initial detection of fraud comes from tips. Reduce "accidental" discoveries by increasing intentional discoveries. You need an anonymous tip line. You need to develop management communication channels (listen to employees). You need to develop an informant program. If you can, reward tipsters. Follow up with informant with results from tips. Maintain regular and consistent controls. Review controls based on prior incidents, including other hotels. When in doubt, check it out. If it just doesn't look right, it probably is not.

placed in the till. If you have departments not following these procedures, suggest them to the department head. The manager will save money that is lost through theft and errors and your internal crime will go down. Second is the enforcement of the developed controls. Employees need to be audited (watched) regularly and their violations addressed. Addressing procedure violations tells the employee that he is being watched and that if he is testing us we are going to catch him. Do not hesitate to modify controls that are lacking or missing. Better to fill the hole late than not at all.

Your Accounting Department or whomever does your internal auditing will help with enforcing these controls and suggesting others.

Accounting

Payroll scams—many large businesses are victims of payroll scams. There are several variations on this, but the most lucrative is to create a fictitious employee. The department head or manager fills out the paperwork to hire an employee who does not exist (or it could be a friend or relative who does not work there). Once the employee is in the system, they clock him in and out every day and have the check mailed somewhere. If this sounds easy to do, think of the controls you can establish to prevent it. Another department (like HR) should meet and enter the employee in the system (can an HR clerk pull off this scam?), have checks picked up in person from another department, random checks of employee time record and duties performed, and camera on the time clock. Other variations of payroll scams are real employees who clock in and out, but do not work, managers who manipulate time records and take a cut of the extra money, employees clocking each other in and out or using job codes with higher pay (if you have an automated system).

Collusion—The most common form of internal theft is where two people from different departments work together to steal. Since a basic control in any money-handling operation is to have two signatures or verifiers of funds, both of those verifiers working together defeats the control. This is common in casinos, but also occurs in any business between employees of one department, employees of opposing departments, and manager and employee. The best control for this is to have a third verifier. If that is not possible, use cameras. In accounting, a common collusion is between a purchaser and an accounts payable clerk (or similar relationship). One buys the product and the other pays for it. Use your imagination: If you buy fruit for the Food Department, how hard would it be to buy a pallet of oranges from yourself and have your friend in accounts payable pay you for that pallet? He could send the check to your cousin's house payable to Darrell Clifton Produce. This is why you need verifiers, such as the receiving clerk who receives the shipment and verifies all the information on the invoice before it is paid.

Credit card fraud—The Payment Card Industry (PCI) Council has made great strides to protect credit card holders. These are not laws, but requirements set forth by Visa, MasterCard, American Express, and others on businesses as a condition of accepting their cards for payment. They are very strict now and if you have not heard of PCI, go to your Controller's office and say, "What in the heck is PCI?" and watch them all jump out the windows. I exaggerate, but only about the windows—they are locked, right? Up until about 10 years ago, any busboy or guest could go through your trash and pull up a receipts containing credit card numbers. This is no longer the case. In fact, your credit card receipts now have most of the credit card number masked and it has to be masked from the time it enters your system until all electronic or paper traces of it are destroyed. However, there is likely someone in your business (probably an Accounts Receivable clerk) who has access to these numbers. If so, this type of theft is hard to prevent. Make sure PCI is followed strictly in your facility.

Identity theft—similar to credit card fraud, a lot of unprotected personal data of customers are floating around your Accounting Department. Several people can access names with addresses and other ID information. Are you doing background checks on every employee?

Charge-offs—Another function of Accounts Receivable is collecting on bills. Denied credit cards, under payments, room damage, and normal bills for goods and services go through this department. Once again, use your imagination to figure out ways to steal if you are an A/R clerk making $12 an hour. Pay me a little extra and I won't report this delinquent bill to the credit card company. Send the money to my house and I will make this bill go away. Send a mattress to my house and just add 1 percent to our bill. Nobody would ever know. Controls like oversight and verification are keys here.

Fake vendors—Just like payroll, it is very easy to set up a fake vendor and pay yourself for services not performed. For example, take window washers. How would an auditor know whether we actually had a vendor washing the windows every month?

Cashiers

Voids—A very common source of extra income for cashiers is a false void or manipulation of voids. The oldest trick in the book is to sell something, collect the cash, void the

transaction, and pocket the money. Most departments will require a supervisor approval for voids, but in the interest of guest service, they are sometimes approved after the customer has left.

Returns—Another old trick is a false return. A cashier grabs an item from stock, scans it as being returned, puts it back in stock, and pockets the money. Sometimes these require approval and sometimes not. Patterns and trends should be watched and audits may catch returns and voids.

Coupons—A cashier obtains a coupon and applies it to a transaction after the customer pays full price. The cashier pockets the difference.

Credit cards—As in accounting, theft of a credit card number is the easiest and most common. It is very hard to trace. Another possibility, especially in restaurants is to overcharge and pocket the difference. A more advanced trick is to use a pocket card reader. Many phones and electronic devices have attachments that do this. Imagine the possibilities.

Restaurants

Besides the common credit card thefts and false voids mentioned in the Retail section of this chapter, there are some losses unique to restaurants. Almost every food server in the world takes the guest's credit card to the back room to process the payment. That food server has temporary possession of the credit card number, the security code from the back, and even the zip code from the customer's driver's license used to verify many credit card thefts. Unfortunately, the guest does not notice the scam until he gets his statement. The credit card company will rarely investigate these crimes and the hotel will never know about it.

Even with PCI rules (credit card company compliance) protecting credit card numbers left around on receipts, technology has made it easier for nefarious frontline employees to obtain credit information. Magnetic and RF card readers can be attached to cell phones or other pocket-sized devices on a food server. Imagine a waiter swiping the customer card on his iPhone on the way to the cashier. How would anyone know? Few controls will mitigate this type of crime. One option is to limit cell phones and other devices while at work. Otherwise, you will have to wait for a report from the guest or possibly the card company that you can investigate. Camera patrols and audits may catch this behavior.

Another popular employee scam is over-charging on the bill. If the server acts as the cashier, then it is a simple case of adding an amount to the bill or entering a higher amount on the authorization and pocketing the difference. If the waiter is not the cashier, he may just add extra items to the bill to raise the total and increase the gratuity. This is more likely in large groups where the payer is not likely to verify the charges on the bill.

A final scam for you to look at is the food cashier who works in a snack bar or deli-type food outlet. Guests often use credit cards in these establishments but are likely not to leave a tip. The guest presents his card, the cashier prints the ticket for the amount, and the customer signs it, leaving the tip line blank. After the guest leaves, the cashier adds a couple of bucks to the tip line and re-authorizes the amount in the register. The cashier pockets the tip amount. The guest is likely not to notice on his statement that he spent $14 instead of $12, so nobody finds out.

Receiving

Receiving has many points in the process where theft can occur. This area generally encompasses the dock, storage areas, and any place where goods are taken into the property. Receiving is where the Purchasing Department connects with the Food Department and other users of these purchased items. As we have discussed throughout this book, theft is most likely to occur when cash and merchandise change hands. Because this is the main function of this department, controls need to be created, followed, and enforced strictly to protect the assets.

The basic process of receiving goes like this. A department, such as Food, places an internal order for more items. Purchasing places the order with the outside vendor. These orders are sent to the dock where they are used to verify that we received everything we ordered and everything that was delivered was ordered. Those verified deliveries are placed into internal storage where they are again ordered by the department on an as-needed basis. You can see where controls at every step of the process prevent theft if the controls are audited.

Outgoing Theft

One of the most common forms of internal theft does not involve receiving at all. It is usually very easy for employees to obtain merchandise that is in their control, such as meat, liquor, or other valued items. The theft occurs when they try to get it out of the building. Trash is generally associated with the receiving dock because they are in the same part of the building. It is important to keep the trash area separate and its access supervised so that items from the building are not brought out, and received items are not transferred over to, the dumpster for later removal. Security should be present when trash is removed from the locked trash area.

Receiving Theft

Merchandise is most vulnerable after the receiver has verified that all items on a packing slip have arrived. Now the property is owned by the company and in the possession of the person moving and storing it. A trash diversion as described previously is common here. Simply grabbing a bottle of liquor and putting it in a locker, delivering a case of extra meat to your friend in the kitchen, or even consuming a six-pack while working can easily go undetected here. Security patrols and audits are good deterrence, but an additional control of having the internal store receive the items from the dock is better. The store's supervisor or audit control should be doing inventories to make sure that what we think we have is what we have. Do not wait until three cases of tequila come up missing from storage to learn how the process works in your hotel. Sit down with the Purchasing Manager or controller to understand the safeguards already in place and to make sure they are adequate.

False Orders and Return Thefts

A slightly more complicated theft is the false order. The receiving clerk says we are all out of steak so he has Purchasing place the order. When the steak arrives, he can do several things. One is he can receive it, sign the driver's paperwork, and throw it in the back of his truck. Two, he can receive it, signing that it arrived and was placed into inventory, and then take it. Three, after receiving it, he can fill out a return slip that it was bad and had to go back, and then steal it. All of these thefts can be caught in the audit process, but can sometimes take weeks to process. By that time, everyone has forgotten about the delivery and because they cannot find the stuff, they just chalk it up to a mistake. Dual controls or a second signature help prevent these problems.

Lost Merchandise

Not all losses in Receiving are intentional. Items are lost or misplaced regularly. Security may or may not get involved in investigating or even mitigating these losses until it reaches a certain dollar amount and someone wants some answers. So, it behooves us to make sure controls are in place to protect against loss, and that those controls are strictly followed. You are correct in that Receiving management and Accounting are more responsible, but they may not see the vulnerabilities that you would see in an assessment of that area.

Do not wait until the big investigation to learn the process. Right now, there are deliveries being made without invoices or signatures, receivers signing without verifying, and shipments not being fully opened and verified. To make it worse, nobody is reporting these losses. They will probably write them off as unknown losses or as items consumed.

I hinted at some of these controls previously, and the department knows which work best, but you may have to help enforce them. This is part of the job of protecting assets.

Housekeeping

Guest-room attendants normally do not handle cash, so internal theft comes in the form of guest property or company property. Strict lost and found and key control policies are important here.

Security

Yes, security officers steal also. Collusion is one common way because Security is often used as the verifier on transactions and they see how all the processes work. Security also has the ability to take from lost and found or make false returns on property. Another one that I have seen too often by officers is a "drunk roll." An officer may accompany an intoxicated guest to his room and then take the guest's money without him knowing.

There are many other internal theft opportunities. If it is possible, someone will find it. The best way to prevent it is with strong internal controls. Keep an eye on other properties. If someone thinks of a way to steal something at another hotel, he or she is bound to try it at yours—or maybe already has.

BACKGROUND CHECKS

So which departments should have background checks on their employees? This is a trick question. And the answer is, all of them. I have seen many hotels that decide the only employees at risk of stealing are Security, housekeepers, and maybe managers. Even if that were true, stealing is the least of our concerns. First, any employee can steal—kitchen workers, receivers, cleaning staff. Second, workplace violence, sexual harassment, drug sales and use, and even poor work performance can be larger risks and create more losses for the property than simple theft. Any employee can participate in these illicit activities, so it is not logical to pick and choose who will have their history investigated.

Many organizations task the Security Director with doing background checks for all employees. If you do this, you know how time-consuming it is. I strongly recommend finding a contract provider to do this for you. It is well worth the price to have an outside company do your background checks. Criminal history is important and you need to check each state in which the applicant lived. This is time consuming and may be costly. This will actually cost you less if you compare like services. The background company knows what and where to check, but make sure the service includes what you want. Consistency—a common theme throughout this book—is key to your fair hiring practices. Imagine trying to defend why you spent hours checking the background of a person of one race, then spent days on a person of another race.

Timing of background checks is just as important as the complexity. In the last century, when a background check required a lot of legwork, many organized crime rings knew how to take advantage. Groups of immigrants from Mexico and Asia, knowing that background checks from their native countries took longer or were almost impossible, would come into a hotel filling those difficult-to-hire housekeeping positions. In cities where hotels were being built at an incredible rate, such as Las Vegas, managers needed housekeepers in quantity and they needed them immediately. They would hire them first, and worry about the background check later. Housekeepers clean about 16 rooms a day and have access to others, so 10 housekeepers in one day could "clean up" 200 rooms and be out before the background check even started.

There are two morals to this story. One is that backgrounds should be completed before an employee starts working. Second is the hiring of immigrants. Legal immigrants go through a long process of obtaining a work visa or resident alien status so they can work legally in this country. Therefore, they should have some work history in the United States, even if it was under-the-table or as a student. If they have a Social Security number, it should be traced to determine if it was newly issued or whether someone else may have had it before. Once again, this is a complex issue and should be given to experienced professionals.