Brad Bonnell, Principal
Hotel Security Group, LLC

Salvatore Caccavale, Principal
Global Hospitality Security Solutions, LLC

Hospitality Fraud Risk Management: The 5% Solution

Hospitality and restauranteur executives often (mistakenly) view some losses as *part of doing business* and there are no controls to minimize these losses. There are, however, methodologies that will shrink these forfeitures in a hotel's P&L statement when applied and embraced as the new method of conducting business and provide a healthier profit.

Losses may be identified (or overlooked) as: abuses of workers' compensation claims, general liability claims, other fraudulent insurance claims, travel and entertainment fraud, misuse and abuse of rewards programs, revenue management swindles, embezzlement, online booking scams, and embellishment of expense reports/accounts, to highlight a few categories.

Evidence of the varying characteristics of hotel and restaurant fraud are underscored in
the media ~

An article in The San Diego Tribune points out the arrest of a Hilton Revenue Manager who was arrested for his participation in a $28 million hotel room fraud investment scheme against his employer.

The American Hotel Lodging Association (AHLA) in a March 2017 article reported the industry is impacted by, in part, "*…some 15 million online hotel booking scams occur every year, translating to $1.3 billion in bad bookings….*" The AHLA further wrote, in part, *"...applauds the Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security today for taking another step in raising awareness about the prevalence and significant impact of online hotel booking scams on American consumers…."*

The U.S. Attorney's Office, Northern District of California wrote in their July 2024 release about a former Hilton employee who, in part, *"...According to his plea agreement, (Geoffrey) Palermo admitted he devised a kickback scheme involving contractors to deprive the Hilton hotel's owners of more than $1.8 million in kickbacks that went to Palermo. As part of the scheme, Palermo agreed with one contractor, Adan Roldan, 56, of Roseville, Calif., that Roldan would submit falsely inflated invoices for construction and renovation work at the hotel, that Palermo would* *approve the false invoices, and that Roldan and the second contractor would pay a kickback to Palermo associated with the falsely inflated invoices…."*

A September 2024 article from Transmit Security offers insight on loyalty program fraud, in part, *"…It's 2024. Do you know who is redeeming your customers' loyalty points? Loyalty fraud is on the rise, costing over $1 billion annually for large travel and hospitality companies. One of the many challenges is that 45% of loyalty program accounts are inactive or infrequently used — and this opens the door for fraudsters takeover accounts and redeem points…."*

For hoteliers and restauranteurs with degrees in hospitality and restaurant management, classes on safety, security and fraud are lightly discussed, if at all, leaving the student unaware of elementary steps to combat this type of crime. A rudimentary aspect in constructing a fence around fraud is a risk assessment. Absent a risk assessment, hotel ownership, hotel leadership and above-property leadership are guaranteed to continually experience greater loses.

Karim H. Vellani, President of Threat Analysis Group, LLC, states in his book, *Strategic Security Management, A Risk Assessment Guide for Decision Makers,* 2nd edition, in part, *"…As the security industry grows to not only Include physical security but also information/cyber security, it is incumbent upon today's security directors to focus more on the business side of security rather than the operation side. This is best summarized by the world's leading security association, ASIS – International, in their Chief Security Officer Guideline:*

Today's business risk environments have become increasingly more sever, complex, and interdependent, both domestically and globally. The effective management of these environments is a fundamental requirement of business . Boards of Directors, shareholders, key stakeholders, and the public correctly expect organizations to identify and anticipate areas of risk and set in place a cohesive strategy across all functions to mitigate or reduce those risks. In addition, there is an expectation that management will respond in a highly effective manner to this events and incidents that threaten the assets of the organization. A proactive strategy for mitigation of the risk of loss ultimately provides a positive impact to profitability and is an organizational governance responsibility of senior management and governing bodies…"

Risk Assessments provide a foundation to develop insight and knowledge on prioritizing potential threats of vulnerability and losses to revenue streams. After conducting a deep-dive of exposed weaknesses, the hotelier will classify the liabilities, and develop a written plan to mitigate losses. A leadership approach must be embraced after the written mitigation plan is developed to ensure that all colleagues are understanding of the situation and are making this matter as equally important to other areas of hotel operations.

Using hotel and restaurant experts to develop a Risk Assessment, and to dissect the findings of the Risk Assessment will provide a clearer lens in how to craft a mitigation plan.

The Cost of Fraud

Credible and reliable research by The Association of Certified Fraud Examiners (ACFE) has demonstrated that on average a business in the US will lose 5% of its gross annual revenue to occupational fraud.

The Center for Counter Fraud Studies at the University of Bristol in the United Kingdom found that a hotel in the UK will lose on average 5.5% of gross annual revenue to fraud and that hotels with no fraud risk management program would lose up to 10% of its gross annual revenue.

The Bristol study also found that hotels with a coherent fraud risk management program could reduce annual losses to fraud to approximately 2%.

As previously stated, all too often these losses are written off as the "cost of doing business" which reflects a lack of understanding of strategic fraud risk management.

Strategic Fraud Risk Management

The process of mitigating the threat of occupational fraud begins with an understanding of what motivates the commission of occupational fraud.

Three fundamental components of fraudulent behavior to emerge.

1. The perception of a need.
2. The ability to rationalize their actions. (i.e., Everyone else is doing it! I deserve it! I was unfairly passed over for a promotion! If I get caught, the only thing they will do is fire me or make me pay it back!)

3. The perception of a “risk free opportunity” to commit fraud. The belief that their fraudulent behavior will go undetected.

An enterprise has no control over an individual’s perceived needs or their ability to rationalize and justify their fraudulent behavior.

However, a business can effectively manage and minimize losses to occupational fraud through a proven process of fraud risk management consisting of the following elements which all function to create the perception of risk for those tempted to engage in occupational fraud.

1. **“Zero Tolerance” Policy Statement**: A statement or “standard operating procedure” from the most senior executive articulating that.
    a. All forms of occupational fraud are prohibited to include but not limited to.
        i. Vendor fraud.
        ii. Contractor fraud.
        iii. Conflict of interest.
        iv. Payroll fraud.
        v. Expense Reporting Fraud (i.e., Travel and Entertainment Expense Reports).
        vi. Any unauthorized diversion or conversion of corporate property, goods or services.
        vii. Performance misrepresentation.
        viii. That all associates, vendors and contractors are required to immediately report any suspected fraudulent conduct or activity.

2. **Confidential Reporting Channels.** It is critical that credible confidential reporting channels be provided and that the offer of “confidentiality” is clearly defined and protected in practice.

3. **Data Mining/Exception Reporting**: For example, continuous assessment of the “top ten” associates for travel expenses, over/short reporting, vendor costs, etc. Any financial or performance activity that significantly exceeds the standard rate of deviation.

4. **Scheduled and Unscheduled Audits and Inspections**: “That which is inspected is maintained.” – George S. Patton.

5. **Prosecution**: The consistent reporting of criminal misconduct to the authorities to avoid the perception of selective discrimination. Also, why it is wise to avoid making a “deal” with an offender to repay what they diverted.