Journal of
Hotel & Business Management

Collins, J Hotel Bus Manage 2013, 2:1
DOI: 10.4172/2169-0286.1000105

Case Report Open Access

Safeguarding Restaurants from Point-Of-Sale Fraud: an Evaluation of a Novel Theft Deterrent Application Using Artificial Intelligence

Galen Collins*

Professor, Northern Arizona University, Flagstaff, AZ, USA

Abstract

The purpose of this article is to evaluate a unique theft deterrent application for restaurant point-of-sale (POS) systems developed by Radiant Systems (now part of NCR Corporation), a provider of POS technology to the hospitality and retail industries. This artificial intelligence (AI) application, Aloha Restaurant Guard (ARG), is used with the Aloha POS system (65,000 installations worldwide) and has been deployed in more than 6000 quick service and table service restaurants in the United States and the United Kingdom. The following research question guided this case study: Is ARG effective in theft detection and prevention?

Keywords: Restaurant; Fraud; Point-of-sale; Artificial intelligence; Theft deterrent; Cash scams

Introduction

A fraud survey found that 75 percent of the 459 responding organizations experienced some form of fraud during the prior 12 month period [1]. The Association of Certified Fraud Examiners (ACFE) estimates 6 percent of revenues are lost due to theft by employees and that small businesses suffer disproportionate losses because of limited resources devoted to fraud detection [2]. Most employee theft is never discovered [3].

Employee theft is a serious threat to the success of small businesses, which often have meagre profit margins [2]. The National Restaurant Association (NRA) reported that the cost of employee theft for its members totalled over $8.5 billion in 2007 or 4 percent of food sales. An older NRA study estimated the annual average theft per employee at $218 per employee [4]. These are significant statistics because a restaurant's pre-tax profit margin typically ranges between 2 and 6 percent [5].

Cash is among the assets stolen frequently from employers [6]. Laube [7] maintains that solid cash controls are imperative for restaurants and to never underestimate the lure of quick (illegal) cash and the length that some employees will go to get it. Five percent of employees commit fraud in any situation, 10 percent do not commit fraud regardless of circumstances, and the remaining 85 percent consider committing fraud only if not getting caught or suffering little or no repercussions if caught are possibilities [8].

Employees steal because they can, according to loss prevention experts [9]. Therefore, the most appropriate strategies for reducing theft are detection mechanisms [10]. Researchers and business leaders have the opportunity to use new technology and knowledge for developing tools and processes for combating the debilitating effects of fraud [3].

Contextual Issues

Because restaurants lose significant profits to internal theft, learning how to reduce it is of prime importance [11]. A POS system, a network of cashier and server terminals for coordinating various restaurant activities, provides better operational control than a manual system, standard cash registers with handwritten checks [12]. An employee intent on stealing, however, can successfully circumvent POS system electronic controls [11]. For employees to steal cash, the following must happen [13]:

- Menu items are delivered to the customers.
- Servers (bartenders and waiters), cashiers, or managers manipulate the POS system to intercept all or a portion of the cash payments rendered or to inflate tips from card payments or meal vouchers.

The following describes common cash scams and examples of corresponding counteractive measures using software and procedural actions recommended for the Aloha POS system [13-15]:

- Scam 1: A server reprints the same check throughout a shift and uses it repeatedly for different cash-paying customers. Counteractive Measure: Limit the server's ability to reprint checks to a predefined number.
- Scam 2: A server has a tab voided by the manager under the guise that the customer walked out on the check but in reality paid with cash. Counteractive Measure: Check audit report for servers with a pattern of "comps."
- Scam 3: A server convinces cash-paying customers to order the same menu items in order to reuse checks, a slight variation of Scam 1. Counteractive Measure: Spot check tables and review corresponding server checks for accuracy and order time of menu items.
- Scam 4: A server takes and transfers another server's credit card slip, which has not been closed yet, to collect on the tip. The server must know the other server's login to perform the transfer. Counteractive Measure: Eliminate the ability to transfer checks.
- Scam 5: Having collected cash, a server persuades the manager to void an item off the check (e.g., presents a barely touched entrée) and pockets the value of the item. Counteractive Measure: Managers should only void off items that have not

***Corresponding author:** Galen Collins, NAU Box 5638, Flagstaff, AZ, 86011, USA, Tel: 928/523-7333; Fax: 928/523-1711; E-mail: Galen.Collins@nau.edu

Received June 14, 2013; **Accepted** July 23, 2013; **Published** July 25, 2013

Citation: Collins G (2013) Safeguarding Restaurants from Point-Of-Sale Fraud: an Evaluation of a Novel Theft Deterrent Application Using Artificial Intelligence. J Hotel Bus Manage 2: 105. doi:10.4172/2169-0286.1000105

been produced. The correct process would be to "comp" the item under the appropriate reason code.

- Scam 6: Servers collaborate by transferring commonly ordered items to each other and reprinting checks. For example, server 1 orders a beverage on the system, prints the check, presents the check to the customer, and then receives a cash payment. Prior to closing the check, server 1 creates a separate check by moving the beverage off the current check. Then server 1 transfers the new check with the beverage to server 2. Server 1 closes the check minus the beverage and pockets the amount of the beverage. Counteractive Measure: Managers must approve transfers between servers.
- Scam 7: A server presents a slightly higher, similar check in hope that a cash-paying customer will not closely review it. Counteractive Measure: Track the number of checks that have been reprinted and reopened by servers.
- Scam 8: A server enters an incorrect gratuity total for meal vouchers collected from customers (e.g., tour bus group). For example, a server collects 10 vouchers each with a $2.00 tip value for a total gratuity value of $20.00. The server then enters $200.00 into the system, something that could be easily explained as a benign slip of the finger. Counteractive Measure: Activate payment reconciliation by job code at the end of each shift to identify totals that do not match.
- Scam 9: For identical orders, a server enters only one item then moves it from the original check to newly created seats or checks (split checks). The checks are then reprinted for pocketing extra cash. For example, if two people at the table order the same menu item (e.g., an appetizer that the server has direct access to), the server enters only one menu item into the system, creates a second check for the second customer, transfers the menu item to that check, prints a bill for that customer, and then transfers the menu item back to the original check for the first customer. Counteractive Measure: Monitor check reprints and split checks by server in the audit report.

Auditing Solutions

A key ingredient towards the success of most organizations is the ability to leverage and create knowledge from the data [16]. A survey of chief internal audit executives indicated that the ability to find trends or patterns in large, complex data sets will be the most important skill for auditors in the future. However, new audit processes that use increasingly sophisticated data mining tools will be required [17]. Data mining is the process of extracting valid, novel, and actionable patterns from large data sets by combining methods from statistics and AI with database management. The integration of data mining tools with auditing tools is a relatively new concept making auditing faster and cheaper [18]. Furthermore, many companies report that such auditing solutions detecting fraud early on pay for themselves in a few months [19].

ARG, the first auditing solution of its kind for restaurant POS systems, uses an AI engine to monitor POS data and transactions and to identify fraudulent activities. If a fraudulent behavior pattern is detected, an alert is generated that includes the details of the suspicious transaction as well as a history of any similar behavior.

ARG was conceived in 2008 by the Radiant Systems Innovation Team, which consisted of senior administrators and technicians, to provide an automated auditing solution with real-time transaction intelligence and pattern and trending analytics for quickly identifying potential employee as well as manager theft. About 41 percent of employee theft perpetrators are managers [20].

The ARG product development and management team, with expertise in programming, statistics, data analysis, artificial intelligence, and operations, unveiled the alpha prototype in three restaurants for testing and evaluation in early 2009. Later that year, the beta version of ARG was deployed in 3000 U.S. and U.K. restaurants. In February 2010, the official ARG launch took place.

ARG is provided as a Software-as-a-Service (SaaS) solution, which means that access to the application is on a monthly subscription basis and the subscriber does not have to install the software or acquire any additional hardware to operate the software. POS transactions, polled daily via the Internet, are analyzed by ARG, an "in-the-cloud" hosted application. Exception-based reports with employee-specific actionable data are generated weekly and accessible via a Web portal.

Evaluation Methodology

The case study research approach was used in this investigation. Such research is the most common qualitative method used in information systems research and appropriate when an in-depth evaluation of a novel solution within a real-life context is required [21-23]. The literature, while not extensive, contains specific guidelines for case study researchers to follow. The research methodology followed in this evaluation is based primarily on guidelines developed by [23].

Case study is a triangulated research strategy, which uses protocols or procedures to ensure accuracy and minimize misrepresentations and misunderstandings [24]. Multiple data sources (data triangulation) using multiple methods (method triangulation) provided both a comprehensive picture of what was being investigated and a way to crosscheck information [25,26].

The data collection methods were forum postings, interviews, and document analysis. Information was gathered from three different data sources: ARG users, product managers, and a technology reseller. The results of the analysis were used to the answer the research question: Is ARG effective in theft detection and prevention?

Results

Document analysis

The following case study information on ARG effectiveness, produced and published by Radiant Systems, is from five different restaurant organizations. Evidence of its effectiveness came from three independent restaurant chains, an independent restaurant, and a Burger King franchisee. The sample included 40 quick service and table service restaurants located in the Bahamas, California, Indiana, Louisiana, New Jersey, New York, Virginia, and Washington D.C. in several varieties:

Alicart restaurant group: This company, with seven restaurants primarily in the northeastern United States, has over 900 employees and $75 million in annual revenue. It offers a variety of dining experiences featuring barbecue and Italian cuisines. The installation process took about 30 minutes after a link was sent via e-mail according to chief executive officer Jeffrey Bank. The results of the ARG implementation according to Bank were:

- Fewer clears and voids and tighter controls over bartended activity. ARG revealed tip anomalies, such as a 1$ bartender transaction with a $49 tip.

- Identification of bartenders and managers that required more training on POS controls.
- Streamlined communications and greater focus on theft. Banks clicks on "follow up" and "email" to communicate to his staff when he has questions about particular transactions and gets timely responses. Managers now call in advance when they have excessive voids, transfers, or other suspicious activity.
- A strong theft deterrent, better than cameras.

Nichols restaurant: This is an independently owned casual dining restaurant located in Marina Del Ray, California. It employs more than 25 servers and 80 employees. Owner and operator Jim Nichols was very skeptical that his servers could be stealing from him. The results of the ARG implementation according to Nichols were:

- Evidence of widespread and ongoing theft. One year of data revealed theft by more than 40 percent of the servers. A 12-year employee had stolen as much as $10,000 per year.
- Increased revenue and an improvement in food costs.
- Estimated annual savings of $20,000 to $40,000.

Sahm's restaurants: This company is one of the largest independent restaurant chains in in the Indianapolis, Indiana area. It provides full-service dining as well as catering operations within local business buildings. Sahm's Restaurants generates over $30 million in annual revenue and employs over 120 servers. The results of the ARG implementation according to director of operations Rick McAnally were:

- Confirmed suspicions of fraudulent activity in all the restaurants. Consequently, the ability for servers to discount checks on their own was removed.
- Increased annual revenue of $10,000 to $20,000.
- Effective theft deterrent. It is a valuable tool for stopping theft now and in the future. It has changed the mind-set of employees.

Tsunami: This sushi-bar restaurant, with locations in Baton Rouge and Lafayette, Louisiana, employs 50 servers, bartenders, and cocktail waitresses. The ARG application was installed quickly and with no interruptions to restaurant operations. The results of the ARG implementation according to regional manager Frederick Nonato were:

- Confirmed fraudulent activity. Bartenders were reporting 300 percent tips, an indication of free drink giveaways. Seven servers were caught stealing upwards of $35,000 annually.
- Fraudulent activity decreased and remained low. Employees were running various scams including servers avoiding tipping out bartenders and sushi chefs.
- Food cost and revenue improved immediately.

Interviews

An interview with ARG product managers Blair Beatty and Scott Walton revealed the following (personal communication, May 19, 2011):

- Prior to ARG implementation, audit reports were used to investigate suspicious employee activity. ARG, leveraging artificial intelligence and pattern recognition, quickly identified a significant number of fraudulent transactions never surfaced through the existing audit controls.
- ARG only identifies scams through POS transactional data. A scam, such as a server not placing orders through the POS system but presenting bills to cash-paying customers verbally or via a handwritten check, would not be detected. The integration of ARG with surveillance video, which will expand the scope of fraud prevention and detection, is planned for the future.
- ARG identifies variations of known scams and aids in the detection of new ones, which arise as the POS system evolves and more capabilities are added. The latest scams involve gift cards and loyalty programs.
- Detailed alerts (e.g., who, when, what, frequency, where, etc.) are provided on a weekly basis and used to facilitate discussions with employees suspected of fraud. The alerts are typically first sent to a central audit group or regional manager in a restaurant chain or group or to the general manager or owner/operator in a small organization. Management theft has also been detected by ARG.

An interview with Michael Fodor, vice president of marketing and sales for F&B Management (FBM), a Phoenix-based restaurant technology reseller and Radiant Systems channel partner, revealed the following (personal communication September 6, 2011):

- Most restaurant operators are reluctant to invest in security-related software services because of tight profit margins, low perceived value, and/or an aversion to sales pitches. FBM has achieved a high adoption rate of ARG by offering clients a free assessment called ARG "Reveal." At least three months of transactions are analyzed for fraudulent activities free of charge. Names of potential culprits are withheld until ARG is purchased. In some restaurants, no fraudulent activities were detected.
- FBM clients implementing ARG have typically experienced a three to five percent reduction in food costs. Some FBM clients found the level of theft, ranging up to two percent of food costs, acceptable and chose not to deploy ARG. Others not deploying ARG viewed theft as compensation to keep employees contented.

An interview with Christina Carlson, vice president and controller of Red Robin Gourmet (RRG) Burgers, Inc., revealed the following (personal communication September 20, 2011):

- RRG, a full-service, national restaurant chain with over 400 locations and annual sales in excess of $840 million, implemented the ARG solution in all of its corporate-owned restaurants in 2009. None of the franchise restaurants, which represent roughly 30% of the brand's restaurants, have purchased the solution, however. Why? Some of them do not use the Aloha POS system. Those who do are probably disinclined to use ARG because of its cost (less than $1000 per restaurant per year) relative to the perceived benefits.
- Because ARG generates automated audit information from a central location, fraud is more easily discovered. It provides

employee-specific actionable data with corroborating evidence. It identified cash scams and schemes involving both employees and managers. It also identified shortcomings in process controls, POS settings, and training.

- Radiant Systems has had difficulties satisfying the reporting requirements of RRG, one of the first large, multi-unit chains to adopt ARG. The sheer volume of data occasionally caused weekly reports to be late, although this problem has diminished. Features and functionality have been added to provide greater reporting flexibility (e.g., report data for any set of restaurants for any time period).
- Those utilizing ARG information require training to interpret the findings and to learn how the scams work, some of which are counterintuitive. Evaluation and follow up of highlighted transactions and patterns are time consuming in a large chain, precluding the investigation of every incident. Each incident requires careful review of the underlying documentation. Suspicious events can have reasonable explanations, such as a server that actually received a high tip. Follow up also entails the identification and correction of systemic issues.
- The solution appears to be cost-effective and a deterrent to fraud. RRG has not quantified the impact of ARG on financial performance. Carlson considers this a daunting extrapolation task for a large restaurant organization. Continued use of ARG by RRG, however, will depend on its ability to identify new schemes and a determination of its deterrent value relative to its cost.

Forum postings

The following paraphrased exemplar comments on ARG effectiveness are from anonymous forum postings by restaurant owners and managers at restaurantowner.com, a paid-members only site:

- ARG User 1. While several controls are in place to prevent most of the problems ARG will alert you to, it is much easier to look at the ARG reports than to generate and sift through Aloha audit reports.
- ARG User 2. After the first week of implementation, we estimated $50,000 in lost revenue among our three stores. I fired the general manager at one store who I thought was doing a great job.
- ARG User 3. We had three employees running the "Wagon Wheel" or transfer scam. One server, who transferred the same ice tea nine times in 90 minutes, stole almost $2,000 over a six-month period. A bartender stole almost $6,000 using the same scam. I never expected them to be scamming us. The system is now being installed at all five of my restaurant locations.

Of the 21 forum postings from April 2009 to May 2011, the ones authored by ARG users were all favorable concerning ARG effectiveness. Sixty-seven percent of the postings, however, were authored by non-ARG users primarily seeking ARG product and pricing information and scam details. One non-ARG user, skeptical about the perceived value of the product, asked: "Is it a gimmick or the valuable tool they claim it to be?"

Conclusion

The evidence collected indicates that ARG is helpful or effective in identifying common scams and undesirable employee behaviors, evaluating security levels and controls, and creating an environment of accountability and fraud deterrence. Other case study conclusions or findings are:

- Aloha POS fraud appears widespread in the restaurant types investigated, although in some restaurants ARG revealed no fraudulent activities. Aloha POS fraud appears to be more prevalent and costly in smaller restaurant organizations which often lack the resources, tools, and knowledge to detect and deter fraud.
- ARG is more easily deployed in smaller restaurant organizations because the reporting requirements and assessment of instances are less burdensome.
- The benefits of ARG are more easily quantified in smaller restaurant organizations, making the business case more tenable.
- Adoption of ARG depends on one or more of the following factors: knowledge of fraud, alleged fraud, or suspected fraud, proof that ARG detects and/or deters fraud, the awareness of fraudulent scams and schemes, the impact of fraud on financial performance, perceptions of employee honesty, the annual cost of ARG relative to its perceived value, restaurant profitability, knowledge of and understanding of ARG, and an operator's tolerance level for theft.
- Optimal use of ARG requires an understanding of the fraudulent schemes and the ability to interpret the reports and make actionable recommendations with the appropriate supporting evidence.
- ARG provides a more robust and comprehensive internal control environment, permitting a substantially different restaurant audit approach that allows operators to find the right balance between POS controls and server efficiency.

The traditional POS audit paradigm is outdated and cumbersome and can be costly. ARG demonstrates how AI technology can vastly improve the POS audit process. There is, however, typically a substantial lag between the introduction of a new technology and its adoption in the restaurant industry. Models of uncertain probability maintain that an organization has an incentive to delay adoption because it can gather information as time passes, and thus perhaps avoid adopting an unprofitable technology [27]. Therefore, the long-term success of ARG depends on its ability to adapt to a changing fraudulent-threat landscape, to evolve functionality through systems integration and enhanced features and reporting tools, and to deliver consistent, measurable results. Additional research is required to more clearly validate and quantify ARG's effectiveness in detecting and thwarting fraud in small and large restaurant organizations.

References

1. KPMG (2003) Fraud Survey of 2003.
2. Moorthy MK, Seetharaman A, Somasundaram NR, Gopalan M (2009) Preventing Employee Theft and Fraud. European Journal of Social Science 12: 259-268.
3. Jackson KR, Holland DV, Albrecht C, Woolstenhulme DR (2010) Fraud isn't just for big business: Understanding the Drivers, Consequences, and Prevention of Fraud in Small Business. The Journal of International Management Studies 4: 160-164.
4. National Restaurant Association (1999) Avoiding an Inside Job. Bread & Butter Newsletter.

5. National Restaurant Association and Deloltte (2010) Restaurant Industry Operations Report 2010 Edition. Washington DC, USA.

6. Walsh JA (2000) Employee theft. International Office of Protection Officers.

7. Laube J (2010) Don't Let Theft Happen in Your Restaurant: What Every Independent Operator Should Know About Internal Controls. Restaurant Startup and Growth.

8. Lavery C, Lindberg D, Razaki K (2000) Fraud Awareness in a Small Business. The National Public Accountant 45: 40-42.

9. Greenberg J, Tomlinson EC (2004) The methodological evolution of employee theft research:The DATA cycle. Jossey-Bass, San Francisco, USA.

10. Purpura PP (2002) Security and Loss Prevention: An Introduction. Elsevier Science/Butterworth Heinemann, Boston, MA, USA.

11. Plotkin R (1998) Preventing Internal Theft: A Bar Owner's Guide. BarMedia, Tucson, AZ, USA.

12. Collins GR, Cobanoglu C (2010) Hospitality Information Technology: Learning How to Use it. Kendall Hunt Publishing Company, Dubuque, Iowa, USA.

13. Francis P, DeGlinkta RC (2005) How to Burn Down the House: The Infamous Waiter and Bartender's Scam Bible. Merry Goldentree, publishers, New Orleans, Los Angeles, USA.

14. Radiant Systems (2006) The Aloha Solution to Restaurant Employee Scams. Atlanta, GA, USA.

15. Albright B (2010) Case study: How Much Illicit Cash are Your Employees Pocketing? Integrated Solutions for Retailers.

16. Schmidt C (2011) Lessons Learned in the Design of an Undergraduate Data Mining Course. Journal of Computing Sciences in Colleges 26: 189-195.

17. Hunton JE, Rose JM (2010) 21st Century Auditing: Advancing Decision Support Systems to Achieve Continuous Audit. Accounting Horizons 24: 297-312.

18. Bagga S, Singh GN (2011) Comparison of Data Mining and Audit Tools. International Journal of Computer Science and Communication 2: 275-277.

19. Burleson D (2011) Critical Audit System Features. Burleson Consulting.

20. Association of Certified Fraud Examiners (2006) Report to the Nation on National Fraud and Abuse.

21. Orilowoski WJ, Baroudi JJ (1991) Studying Information Technology in Organizations: Research Approaches and Assumptions. Research 2: 143-169.

22. Merriam SB (1988) Case Study Research in Education. Jossey-Bass Inc., Publishers, San Francisco, CA, USA.

23. Yin RK (1994) Case Study Research: Design and Methods. (1st edn.) Thousand Oaks, Sage Publications, Inc., CA, USA.

24. Stake R (1995) The Art of Case Study Research. Thousand Oaks, Sage Publications, Inc., CA, USA.

25. Gay LR (1996) Educational Research: Competencies for Analysis and Application. Prentice Hall, Upper Saddle, New Jersey, USA.

26. Merriam SB (1988) Qualitative Research and Case Study Applications in Education. Jossey-Bass Inc., Publishers, San Francisco, CA, USA.

27. Doraszelski U (2004) Innovations, Improvements, and the Optimal Adoption of New Technologies. Journal of Economic Dynamics & Control 28: 1461-1480.