CHIP & PIN Technology:

A POS Solution for Restaurants and Hotels

Alecia Douglas
MS. Hospitality Information Management
Hotel, Restaurant and Institution Management
University of Delaware

Abstract

Over the last few decades, the evolution of information technology (IT) in an increasingly competitive environment has been dynamic and unpredictable to say the least. There is no doubt that IT advances have radically altered the way many industries now conduct their business (Ansel and Dyer, 1999). New technologies have served up smart business solutions that have thrust industries to achieve greater levels of internal proficiency in core operational areas. These innovations have also impacted the external business environment tremendously especially at the business to consumer (B2C) level. This paper serves to introduce one such technology, the PIN and Chip smart card, at the forefront of change in the European business environment and the implications for adopting a similar strategy in the United States (US). More specifically, it is aimed at exploiting the use of the technology at the point-of-sale (POS) in restaurants and some instances at hotels as a measure to combat credit card fraud and improve the tarnished reputations of restaurants oblivious to fraudulent activities that occur in their businesses.

Introduction

While it may be asserted that industries in general have been receptive to technological innovations, the saying does not hold true for hospitality and by extens ion, the restaurant industry. Described as 'late adaptors', 'laggards', 'slow' and even ' ultra-conservative' towards IT, restaurants at best are not bereft of technology (HITA, 2003; Ansel and Dyer, 1999). As a matter of fact, Ansel and Dyer (1999) purports that the heart of a restaurant's information technology are robust POS systems. Yet even with advances in this innovation, there is no guarantee that customer interaction, or lack thereof in the case of a fine dining restaurant, with the POS is valid and credible. As a result, the restaurant in some way contributes to fraudulent activities. Interaction in this context refers to the 'moment-of-proof' with the use of the electronic cash as the customers preferred method of payment. Incidentally, American Express (2002) reports that services such as restaurants, bars, and gas stations may be the most vulnerable businesses to criminals by indirectly acting as an 'accessory to fraud.' This assertion is best illustrated through the following scenario.

As the CIO of Secure Enterprises, Jack decides to treat a few of his new international business associates to dinner at an upscale home-town restaurant. Suggested by his secretary as the finest in town and one that truly exemplifies Southern hospitality, Jack looks forward to the evening as the perfect end to a successful day at the office. The secretary was right as Jack and his fellow partners enjoyed the evening with flair and pageantry as the restaurant served up the finest Southern cuisine topped off with the best service. After having dessert, Jack requests his bill and secures payment using the company's platinum credit card. He even leaves a generous tip for his most hospitable attendant.

Several months later, the accounting manager becomes suspicious about a growing list of questionable charges made to the company's credit card, a list that is costing Secure Enterprises $9,000 at last count. Jack couldn't have been more surprised to find out that his well spent evening with his associates a few months ago was the key to the current mayhem. As it turns out, the company's platinum credit card was skimmed by the 'hospitable' waiter leaving the cardholder with the responsibility. It seems as if Secure Enterprises needs a more 'secure' credit card and the once thought of 'finest' restaurant has suffered a blow to its image and reputation at the hands of some dishonest employee. In this scenario, both businesses have been exposed to the world of credit card fraud; the victim, Secure Enterprises and the restaurant, 'an indirect accessory to fraud.'

Credit Card Fraud

It is estimated that in 1998, fraud cost businesses in the United States (US) approximately $400 billion annually according to the Association of Certified Fraud Examiners (ACFE) which represents 6% of an organization's annual revenue or $9 per employee per day (Featsent, 1998). By 2001, credit card fraud in the US rose to US$1,750.5 million up from $1,663.7 million in 2000, an increase of 5.2% (ePaynews.com, 2003). Similarly in the United Kingdom (UK), credit card fraud has been increasing at an alarming rate. Total credit card fraud rose to £411.4 million GBP (Great Britain Pounds) in 2001 up from £317 million in 2000, an increase of 30% (Card Technology Today, 2002). Of this figure, £107.1 million was directly attributed to the use of counterfeit cards which are produced by skimming. Tables 1 and 2 below illustrates the increase in card fraud in the US and UK respectively.

Year	Total Fraud (USD mn)	Online Fraud Rates	Amount of Online Fraud (USD mn)	Offline Fraud Rates
2000	1,663.7	3.0%	823.65	0.07%
2001	1,750.5	2.5%	852.63	0.07%
2002	1,823.7	2.1%	857.85	0.07%
2003	2,373.2	2.5%	1,227.88	n/a
2004	2,664.9	2.4%	1,456.92	n/a
2005	2,745.4	2.2%	1,611.39	n/a
2006	3,028.8	2.0%	1,729.00	n/a
2007	3,212.7	2.0%	1,988.35	n/a

Figure 1. US Credit Card Fraud Statistics, 2000 – 2007

Type of Fraud	GBP million 2000	GBP million 2001	Percent change
Counterfeit cards	107.1	160.3	50
Cards stolen or lost	101.9	114.0	12
Fraudulent use of card details	72.9	95.7	31
Cards intercepted in post	17.7	26.7	51
Fraudulent applications	10.5	6.6	-37.5
Other	6.9	8.0	15
TOTAL	317.0	411.4	30
Losses against	0.162	0.183	13

Table 2 Fraud Losses on UK-issued Cards by Type

The art of skimming is the most prevalent type of counterfeit that involves the copying of genuine data from a magnetic stripe card such as a debit or credit card without the knowledge of the cardholder and replicating that data on to another card(s) as in the case of Secure Enterprise (Card Technology Today, 2002). The process as outlined by Reim (2003) is achieved by 'skim artists' who recruit gofers such as unscrupulous bartenders, waiters or shop assistants that typically find temporary work in restaurants, hotels and retail stores. Their job is to steal information from a customer's credit card such as name, address, telephone number, card number credit limit and PIN number.

The recruit is furnished with a small illicit electronic device known as a skimmer that resembles a pager and can be worn on a belt complete with a scanning slot. By secretly swiping the card in the skimmer, the information held on the magnetic strip is copied to the device and stored until retrieval when it is downloaded and replicated to a counterfeit card complete with security hologram markings. This process takes merely a couple of seconds to produce a counterfeit card and less than a day for the card to hit the streets.

In an effort to control the wave of credit card crime in restaurants, bars and pubs, American Express (2002) has issued a publication on preventing card skimming to the members of the Florida Restaurant Association. This action served as a measure to increase the awareness of credit card crime which may be perpetrated by employees. Similar ly, in the UK, an organization called Card Watch (2002) has issued a counterfeit alert for bars and restaurants reporting that losses from these businesses run into £3 million because of the extensive use of counterfeit cards.

This problem in hospitality stems from the increased use of plastic versus paper as the preferred method of payment at POS and is a net effect from operating in a cashless society. At a time when the focus of hospitality enterprises is on value added benefits for guests (Oder, 2000), it is interesting to note the lack of response towards adopting smart card technology as a business solution. This ‘small wonder’ has had little growth in the US market as it is reported that merely 6% of total financial credit cards are based on smart card technology representing only 12 million credit cards (RFID, 2002). Yet the capabilities of leveraging this technology are endless and it may prove to be the answer to card fraud at POS in addition to capitalizing on potential marketing power thus creating value for the patrons of restaurants, hotels and other services.

SMART Card Technology: The CHIP & PIN

The use of smart card technology across Europe today continues to flourish at an increasing rate than here in the United States (Outwater, 2001). Similar in size and shape to a credit card, smart cards will store and process information on an integrated microprocessor chip located within it and is made available in the form of an ‘intelligent’ card or as a ‘memory’ card (Allen and Kutler, 1997). The intelligent card contains a processing unit that securely stores information and facilitates decision making in addition to read/write capabilities thus allowing new information to be added and processed. On the other hand, memory cards contains a predetermined stored value which the user can ‘spend’ for example at a pay phone, retail store, vending machine or other such related transaction.

Traditionally, Europe has been at the forefront of chip technology from as early as 1971 when Roland Moreno, a Frenchman obtained the first patents for the chip developed in 1971 by Ted Hoff, an Intel Corporation scientist (Allen and Kutler, 1997). With a vision to incorporate chip technology with microelectronics, Moreno’s ingenuity evolved to form the backbone of European society. It was under this guise that the government of the United Kingdom and the financial sector along with approval from the retailers embarked on an aggressive campaign to rid the country of credit card fraud (Card Technology Today, 2002). This strategy is fueled by the main driver of change which is the desire to cut down on fraud.

By using smart cards, the financial sector in the UK strongly purports that the technology will not only help to crack down on card fraud but also offer opportunities for value added services such as retailer’s loyalty programs and secure access to the Internet and online purchasing (Card Technology Today, 2001). It has been argued that any attempt at counterfeiting a smart card would be challenging and extremely costly for the skim artist therefore making the process almost impossible to achieve. As such, the main line of defense which is to reduce card fraud has been met with formality and co-operation from numerous players so much so that a global card specification has been developed by Europay, MasterCard, and Visa (EMV) to provide internationally accepted standards for smart cards and smart card terminals used for debit/credit payments made by a smart card (Card Technology Today, 2001). To this end, the strategy choice was to implement a global initiative starting with the UK on a more secure method of payment, that of the Chip and PIN technology.

Simply put, Chip and PIN is a secure smart card payment system developed to help prevent credit card fraud. With the embedding of a microchip into a debit or credit card, the technology will provide high secure memory and processing capabilities in addition to holding the same data as that on a magnetic stripe (chipandpin.co.uk, 2003). The accompanying security feature, the PIN, is the familiar four-digit personal identification number either assigned to or chosen by the cardholder. The logic behind the PIN safety feature is twofold. First, it shifts the responsibility of identifying the cardholder away from the point-of-sale staff and second, it reduces the time spent by the customer at the register. By entering the four-digit code the verification process would be reduced as against accepting a signature at the POS which takes a longer time.

The implementation of the technology started with a town trial in Northampton, UK during Spring 2003, and will be rolled out around the UK over the next 21 months. It has been estimated by APACS (Association for Payment Clearing Services, UK) that over the next two to three years, all 100 million UK debit, credit and charge cards will be re-issued with Chip and PIN capability (APACS, 2002). By January 2005 the majority of cardholders will have received new chip cards and the retailers are expected to have smart card terminals installed. The total costs of implementing the PIN program are estimated to some £1.1 billion, spread over the next two to three years. Most European countries are about to issue cards to the same specification, and over time there will be increasing use of these cards around the world.

This presents a solid case for retailers and service businesses especially hospitality enterprises in the UK to adapt this technology as the ramifications will be costly. For hospitality businesses that accept card payments, it is expected that the knowledge and the systems that will enable the Chip and PIN system will be implemented and will revolutionize the way transactions are performed and services managed (chipandpin.co.uk, 2003). Alphameric Hospitality (2003) further implies that the penalties for noncompliance for hospitality businesses in the UK will be grave as at the end of 2004 the international card schemes will change the liability for card fraud to sit with the party who has the weaker security system. As a result, if there is a case of fraud and only one party has upgraded their system, that party will be protected from liability for fraud. Otherwise if both parties have upgraded their systems the retailer will be protected if there is a fraudulent transaction. Businesses that refuse to adopt this system will run the risk of attracting card criminals who will target the weakest link.

The view to implementing this technology in the western hemisphere however is aloft as there are some who conc eive that introducing smart cards as a fraud control measure has never been a clear cut business decision (Card Technology Today, 2001). Additionally, others baulk at the thought of replacing the magnetic stripe card with the microchip embedded smart cards. While the strategy to implement Chip and pin technology in the UK was a concerted effort, it is apparent that the US will adopt a different strategy if there is a serious drive to adapt smart card technology. According to a report on smart cards in US banking from Celent (2001), smart cards are unlikely to find their way into the wallets of the masses without a mandate for conversion from the card consortiums. The report alludes to the fact that smart cards are expected to languish in the US market unless there is a consensus from a major banking consortium to transition in unison.

From the review of literature some benefits to the technology include its data storage capacity as against that of the magnetic stripe card (Allen, Kutler, 1997). The fact that higher levels of security is a benefit is no myth as the cards prove to be more tamper resistant and difficult to replicate when compared to its rival. Additionally, smart cards will not wear out as easily as magnetic stripe through contact or friction and it is not susceptible to damage if passed through a magnetic field. Another benefit is the fact that with the microchip technology, advances in biometrics can easily be facilitated to include a fingerprint or even voice recognition (Card Technology Today, 2001). Presently, the benefit of multi-application appears to be the factor that will drive the implementation of the technology in the US as businesses are more capable of providing far more services that simple credit or payment service such as retailer loyalty schemes or electronic purse.

It is anticipated that if the US were to adopt smart card technology in the manner that the UK has, the strategy will be to capitalize on the potential benefits rather than as a solution to credit card fraud. Smart card will be adopted in the US for such reasons as improving e-commerce security, facilitating loyalty schemes and providing multi-application features (Card Technology Today, 2001). To that end, card companies such as Visa launched the Smart Visa platform in 2000 with an intention to provide member banks with a foundation of prepackaged solutions that can be customized to fit their individual strategies for issuing smart cards to consumers (Visa.com, 2003).

Likewise, MasterCard released its "*One*SMART™" card representing a comprehensive approach to a four-point delivery system that includes market-ready technology solutions, end-to-end implementation consumer value proposition and global marketing initiatives (Mastercard.com, 2003). Added to the list of card providers with smart card solutions is

American Express which offers the technology with a PIN and magnetic strip. The main purpose of 'Blue' by American Express is to facilitate a secure environment for online purchases for Blue cardholders. The solution requires an additional smart card reader that can be connected to the user's machine by using either a serial reader or a USB reader.

Recommendations for Implementation

With vendors and card companies in the UK forging ahead in the wake of increased demand arising from the mandatory compliance to Chip and PIN, restaurateurs will need to follow some guidelines that will ensure for a smooth transition for employees and customers alike. The same rules would also apply for US businesses, namely the restaurant in the above scenario. Firstly, all POS systems must be upgraded to be compatible with chip technology in addition to existing software and hardware components of the information system. The business should conduct a situation analysis to determine if there are any internal problems that currently contribute to problem of credit card fraud as perpetrated by employees. In addition, the restaurant must engage in proper training of the new system and conduct test runs to see the effect of the system on performance and guest satisfaction. From this process, it can be determined if there is a need for a system wide change in the service delivery process and if so, the measures that should be taken to retrain employees as well as to effectively communicate the reasons for the change to the guest.

Other recommendations for hotels and restaurants that offer loyalty programs is that they must attempt to capitalize on the technology in the infancy stages so that as it evolves, the business is flexible enough to evolve with the technology as well. By doing so, the entity can attest to the fact that one of the key value drivers in the bus iness is the use of Chip and PIN technology integrated with a CRM solution to enhance the guest experience and reward. It is also essential for the restaurant to know their guests in order to assess the most preferred method of payment. If it is determined that credit cards are preferred for payment, then the opportunities exist for collaborations with card issuers to combine loyalty points for additional value adding benefits. As the guest is a part of the service, the hospitality entity must also communicate the change to them and as such they too must be trained about the new system. One method of accomplishing this is by training employees to impart their knowledge to the guests of the new system. Another method is that a targeted email to credit card users from the restaurant's database could be sent informing the guests of the new system and the benefits for them. Email addresses could be obtained from guest comment cards. Another important recommendation addresses the fact that the technology solution employed should be built on an expandable platform in addition to facilitating interoperability and the card scanner or reader should be compliant with the EMV global specifications.

Vendor and Supplier Recommendations

Key players such as IBM that have been at the forefront of POS technologies must continue on an innovative track and move beyond the traditional point-of-sale solutions by establishing strategic partnerships with card issuers and retailers. One such effort is the collaboration between Visa and IBM UK to develop EMV compliant solutions for large retailers (IBM.com, 2002). The first benefactor of this initiative is Safeway, a leading supermarket retailer with 500 stores in the UK. With the planned implementation, Safeway will become the first major UK retailer to be fully compliant with the EMV chip card technology.

Initiatives like the aforementioned need to be adopted for the US market for multi-application terminals. These terminals provide the opportunity of penetrating new vertical market segments, for example, electronic gift cards are capable of promoting novel opportunities in traditional environments such as restaurants (Card Technology Today, 2003). Further, with a global thrust towards value added payment applications, the demand for multi-application terminals is increasing.

Vendors like IBM should also take advantage of the capabilities of organizations such as the EMV as the possibilities of gaining competitive advantage through extensive environmental scanning activities are evident. The EMV has given companies such as Global Marketing at Verifone opportunities to predict where the industry will be in the next three to five years and to develop solutions to meet the changing payment landscape (Card Technology Today, 2003). Other possible breakthroughs include developments in ePOS terminals that are designed for international specifications and will provide global leverage for IBM as the Chip and PIN sweeps across Europe, Asia and eventually the rest of the world. By doing so, IBM would have created a firm foundation built on smart card terminal technology which is constantly in the re-engineering process and so would support continuous improvement and total quality management (TQM). Competitors having not realized the full potential of this technology will essentially be playing 'catch up' while retailers and services would have IBM as a household name.

With the impending change in the service process especially for fine dining restaurants where payment will be conducted at the table instead of a cash register, business solutions will need to be developed. One such solution could be wireless hand held POS devices that have the capability of taking the server through a step by step routine from taking the order to checking when each course will be ready to securing payment. The device could feature a smart card reader for the guest to insert his/her card for payment.

Conclusion

Whether the strategy is to adopt the technology for the sole purpose of reducing credit card fraud or to leverage the potential benefits of Chip and PIN for marketing efforts, two things are evident from the research. The first is that there is an expectation that the technology will result in the reduction of credit card fraud perpetrated by skim artists using counterfeit cards obtained from unscrupulous servers in restaurants and hotels. The second is that B2C solutions can if be greatly enhanced if the technology is adopted and used to the advantage of services such as restaurants and especially hotels where guest loyalty programs and customer relationship management are the focus as previously mentioned. Consequently, the implications for hospitality can only be maximized if there is an effort to place pressure on the suppliers and vendors of the technology including the credit card providers.

The challenge for hospitality is to influence regulation that would be favorable to the industry by actively lobbying governments and regulators on key issues driving change in the environment for example, Chip and PIN that will shape the future of the industry. This action illustrates the power and rules dimension which suggests that the business has a choice between trying to control its environment or reacting to it (Olsen, Tse and West, 1998). As a result, the industry would essentially try to control the environment through organizations such as the National Restaurant Association (NRA) and the American Hotel and Lodging Association (AHLA). This initiative can be achieved by creating a demand for technological solutions that will not only process credit card transactions, but also transactions for private label cards including gift cards, stored value cards, discount cards, family cards, loyalty cards and another payment types (Oder, 2000). Additionally, Oder (2000) emphasizes that hospitality enterprises are demanding systems that guard against internal attacks from trusted employee fraud.

References

Alphameric Hospitality (2003). How will chip and pin affect the hospitality business? Retrieved May 10, 2003 online from www.crown.uk.com/chip.htm.

American Express (2002). Preventing credit card skimming: a business owner's guide. Retrieved May 10, 2003 from www.flra.com/news_skimming.pdf

Ansel, D., & Dyer, C. (1999). A framework for restaurant information technology. Cornell Hotel and Restaurant Administration Quarterly, 40(3), 74-84.

Association for Payment Clearing Services (APCA), (2002, February). Press Release. Retrieved May 10, 2003 online from www.apacs.org.uk/downloads/pinpro802.pdf.

Allen, C.; Kutler, J. (1997). SMART cards: seizing strategic business opportunities. McGraw Hill.

Card Technology Today (2001, April). Visa redoubles efforts to get smart payment cards into circulation. Card Technology Today, 2001 (April) 13-14.

Card Technology Today (2001, November/December). Can US banks afford to wait for smart cards? Card Technology Today, 2001 (November/December), 14-15.

Card Technology Today (2002, May). UK banks act to check rising card fraud. Card Technology Today, 2002 (May), 14-15.

Card Technology Today (2003, April). Turning the POS into a Point of Profit. Card Technology Today, 2003 (April), 10-11.

Card Watch (2002). Counterfeit Alert! Bars and restaurants. Retrieved May 10, 2003 from www.cardwatch.org.uk/pdf_files/counterfeitbars.pdf

Chip and PIN Programme (2003). The official UK chip and pin website: About chip and pin. Retrieved from www.chipandpin.co.uk

Featsent, A. W., (1998). Preventing fraud: don't get suckered. Restaurants USA. Retrieved May 21, 2003 from www.restaurant.org/rusa/magArticle.cfm?ArticleID=288

Gin, J. (2003, February, 4). Identity thieves may have your number; check statements, mail, credit reports. The Times-Picayune Publishing Company. Retrieved May 10, 2003 from www.lexisnexis.com.

Hospitality Technology, & HITA (2003). Strategic uses and future directions of IT in the lodging industry. Hospitality Technology Supplement 2003.

IBM (2002, September). Safeway and IBM at the forefront of bringing chip card enabled checkouts to the UK. Retrieved May 10, 2003 from www-.ibm.com/industries/retail/doc/content/news/pressrelease/255499101.html

Oder, D. J. (2000). The future of electronic payments – from paper to plastic and beyond. Hotel Online Special Report. Retrieved April 18, 2003 from www.hotel-online.com.

Olsen, M.; West, J.; Tse, E. (1998). Strategic management in the hospitality industry 2nd Edition. John Wiley and Sons, Inc.

Outwater, M. H. (2001). Smart cards in US banking: is the chip hip? Report published by Celent. Retrieved May 20, 2003 from www.celent.com/PressReleases/20011018/SmartCard.htm.

Reim, A. (2001). Cybercrimes of the 21st century: crimes against the individual – Part 1. Computer Fraud and Security, 6(1), 13-17.

RFID Journal (2002). US smart card use up sharply. RFID Journal. Retrieved May 20, 2003 from www.rfidjournal.com/article/articleprint/92/-1/1/