



If it fits, it ships.®
 Get your **free Shipping Kit** now. [Get Shipping Kit >>](#) **UNITED STATES POSTAL SERVICE®**
*For mailable items up to 70lbs. Visit usps.com for details. ©2010 USPS. Eagle logo, shipping box trade dress and letter carrier uniform are USPS trademarks.
 Priority Mail® Flat Rate Boxes

SEARCH: [GO!](#)

What's New	Randomizer	Hot 25	FAQ	Odd News	Glossary	Newsletter	Message Board
----------------------------	----------------------------	------------------------	---------------------	--------------------------	--------------------------	----------------------------	-------------------------------

[Home](#) > [Crime](#) > [Crime Warnings](#) > [Card Sharks](#)

[Contact Us](#) | [Submit a Rumor](#) | [Submit a Photo/Video](#)

CATEGORIES:

- [Autos](#)
- [Business](#)
- [Cokelore](#)
- [College](#)
- [Computers](#)
- [Crime](#)
- [Critter Country](#)
- [Disney](#)
- [Embarrassments](#)
- [Fauxtography](#)
- [Food](#)
- [Glurge Gallery](#)
- [History](#)
- [Holidays](#)
- [Horrors](#)
- [Humor](#)
- [Inboxer Rebellion](#)
- [Language](#)
- [Legal](#)
- [Lost Legends](#)
- [Love](#)
- [Luck](#)
- [Media Matters](#)
- [Medical](#)
- [Military](#)
- [Movies](#)
- [Music](#)
- [Old Wives' Tales](#)
- [Politics](#)
- [Pregnancy](#)
- [Quotes](#)
- [Racial Rumors](#)
- [Radio & TV](#)
- [Religion](#)
- [Risqué Business](#)
- [Science](#)
- [September 11](#)
- [Sports](#)
- [Travel](#)
- [Weddings](#)

[E-mail this](#) [Share this](#)

Card Sharks

Claim: Hotel room keycards are routinely encoded with personal information which can be easily harvested by thieves.

FALSE

Examples:

[Collected via e-mail, 2003]

Southern California law enforcement professionals assigned to detect new threats to personal security issues, recently discovered what type of information is embedded in the credit card type hotel room keys used through-out the industry.

Although room keys differ from hotel to hotel, a key obtained from the Double Tree chain that was being used for a regional Identity Theft Presentation was found to contain the following the information:

- Customers (your) name
- Customers partial home address
- Hotel room number
- Check in date and check out date
- Customers (your) credit card number and expiration date!

When you turn them in to the front desk your personal information is there for any employee to access by simply scanning the card in the hotel scanner. An employee can take a hand full of cards home and using a scanning device, access the information onto a laptop computer and go shopping at your expense.

Simply put, hotels do not erase these cards until an employee issues the card to the next hotel guest. It is usually kept in a drawer at the front desk with YOUR INFORMATION ON IT!!!!

The bottom line is, keep the cards or destroy them! NEVER leave them behind and NEVER turn them in to the front desk when you check out of a room. They will not charge you for the card.

[Collected via e-mail, 2005]

Just received this and thought it was worth sending around — with so much identity theft going around, makes sense!!

Remember this for the future:

You know how when you check out of a hotel that uses the credit-card-type room key, the clerk often will ask if you have your key(s) to turn in...or

there is a box or slot on the Reception counter in which to put them? It's good for the hotel because they save money by re-using those cards. But, it's not good for you, as revealed below.

From the Colorado Bureau of Investigation:

"Southern California law enforcement professionals assigned to Detect new threats to personal security issues, recently discovered what type of information is embedded in the credit card type hotel room keys used throughout the industry.

Although room keys differ from hotel to hotel, a key obtained from the "Double Tree" chain that was being used for a regional Identity Theft Presentation was found to contain the following the information:

- a.. Customers (your) name
- b.. Customers partial home address
- c.. Hotel room number
- d.. Check in date and check out date
- e.. Customer's (your) credit card number and expiration date!

When you turn them in to the front desk your personal information is there for any employee to access by simply scanning the card in the hotel scanner. An employee can take a hand full of cards home and using a scanning device, access the information onto a laptop computer and go shopping at your expense.

Simply put, hotels do not erase the information on these cards until an employee re-issues the card to the next hotel guest. At that time, the new guest's information is electronically "overwritten" on the card and the previous guest's information is erased in the overwriting process. But until the card is rewritten for the next guest, it usually is kept in a drawer at the front desk with YOUR INFORMATION ON IT!!!!

The bottom line is: Keep the cards, take them home with you, or destroy them. NEVER leave them behind in the room or room wastebasket, and NEVER turn them in to the front desk when you check out of a room. They will not charge you for the card (it's illegal) and you'll be sure you are not leaving a lot of valuable personal information on it that could be easily lifted off with any simple scanning device card reader. For the same reason, if you arrive at the airport and discover you still have the card key in your pocket, do not toss it in an airport trash basket. Take it home and destroy it by cutting it up, especially through the electronic information strip!

Origins: The notion that hotel key cards are routinely encoded with all sorts of personal information (thus making them dangerous should they fall into the hands of identity theft scammers) began in 2003 when an overzealous detective with the Pasadena (California) Police Department sent around a warning e-mail based on a misunderstanding of something she'd heard:

This urban legend can be traced back to an e-mail that a detective from the Pasadena Police Department sent out more than four years ago.

"One of our investigators was at a meeting with other fraud detectives," says Ronnie Nanning of the Pasadena police. "Someone there happened to say that they heard that it was possible to put this information on this key card."

The detective notified other detectives as a "heads-up" to the possibility. That information was shared with others in the police department, who then passed it on before the risk could be evaluated, she says. It took on a life of its own.

Nanning says her department contacted major hotel chains at that time, and "were told time and time again that this was not the policy."

The misinformation wave created by the detective's erroneous e-mail was so large the Pasadena police eventually issued a [retraction](#) explaining that the information it contained was based upon a single incident from several years earlier, and that they had no evidence the warning reflected a current or ongoing issue:

On October 6, 2003, Detective Sergeant Kathryn Jorge of the Pasadena Police Department received information from a group of Southern California fraud detectives who had formed a fraud investigations network through a local internet carrier. One of the members of this group from another San

Gabriel Valley agency reported that in an investigation that he was personally involved in, he came across a plastic hotel card key from a major hotel that had personal information that could potentially lead to identify theft and fraud. This information included names, addresses, length of stay, and credit card numbers. This detective took the precautionary measure of notifying the detectives in the network prior to seeing if this practice was standard in the industry.

As the investigation into this potential fraud risk continued, this information was shared with other members of the Pasadena Police Department and personnel chose to share this information with others before we could correctly evaluate the risk. This has caused a chain reaction of probably thousands of people being given this information before the risk was evaluated thoroughly.



As of today, detectives have contacted several large hotels and computer companies using plastic card key technology and they assure us that personal information, especially credit card information, is not included on their key cards. The one incident referred to appears to be several years old, and with today's newer technology, it would appear that no hotels engage in the practice of storing personal information on key cards. Please share this information with anyone who has a concern over the initial information send out to others as a precautionary measure.

There was never the intent of the Pasadena Police Department to forward this information to others before the risk was evaluated. The information was forwarded by individuals as a possible precautionary note of interest only.

Hotels generally have no practical or functional reason for wanting to encode customers' personal information on their room key cards; most of them have databases that store the very same customer data, so they have no reason to encode anything more than basic information (e.g., room number, access code, activation and expiration dates) on the key cards themselves. In fact, even that basic information isn't really stored directly on the cards themselves – it's encoded as a serial number which a door lock read, decodes, and uses to determine whether or not the inserted key is authorized to open it. We verified all of this with the Vice President of Loss Prevention for the Hilton hotel chain, who told us:

Certainly, modern security systems are sufficiently sophisticated that personal identifying information "could" be encoded onto hotel card-keys. To do so, however, would be pointless and would create additional work (and expense). Hotel card keys would, obviously, contain a "serial number" (to identify the individual physical card); a room number that the card is programmed to open; and the beginning and ending dates for which the card is valid. But there would be no basis whatsoever for the card to contain the occupant's name or credit card information. The VP has personally verified with their 3 access control system providers that their card keys do not contain personal identifying information.

A contact with considerable experience in hotel operations similarly told us:

I have worked as a desk clerk for three hotels: Holiday Inn, Best Western and the Howard Johnson. In all cases, the TESA lock system (key-card) was not connected to the front desk computer in any way. To create a key for a guest, we typed the room number, the number of nights of the stay and how many keys we wanted to create. That's all the information that was recorded. There was no way of encoding any other information.

I would be most surprised to find out that any hotel encoded other information on the key-card. Current technology allows for guests to quick-checkout with the pay-per-view movie system on the TV, so there isn't any need to have more than the room number and length of stay on the key-card.

Even in cases where hotel key cards can be used to purchase goods and services (e.g., at a resort complex such as Walt Disney World or on cruise ships), guests' credit card information is not encoded on the cards themselves; the cards simply contain a flag indicating that the guest has a credit card on file with the resort and is authorized to charge purchases to his room.

In January 2006, *Computerworld* investigated the key card rumors by collecting and examining over 100 hotel card keys and found no personally identifiable information on any of them:

As part of a Computerworld investigation into the allegations, reporters and other staff members who traveled last fall brought back 52 hotel card keys over a six-week period. The cards came from a wide range of hotels and resorts, from Motel 6 to Hyatt Regency and Disney World. We scanned them using an ISO-standard card reader from MagTek Inc. in Carson, Calif. — the type anyone could buy online.

We then sent the cards to Terry Benson, engineering group leader at MagTek, for a more in-depth examination using specialized equipment. MagTek also gathered cards from its own staff. In all, 100 cards were tested.

Most cards were completely unreadable with an off-the-shelf card reader. Neither Benson nor Computerworld found any personally identifiable information on them. Based on these results, we think it's unlikely that hotel guests in the U.S. will find any personal information on their hotel card keys

We also purchased our own MagTek card scanner and have scanned several dozen magnetic room keys we acquired during our various hotel stays over the last few years and likewise found not a single key with any personal information stored on it.

A somewhat related but distinctly different theft [scheme](#) involves crooks' stealing credit card information (through other means) and then encoding that information onto hotel keycards:

It never fails. Emptying your pockets after a vacation or business trip, you fish out the hotel key cards you've forgotten to return. In fact, hotel key cards are unwittingly taken so often that thieves are taking advantage of public and industry complacency on the issue by storing stolen credit card information on the cards and using them like debit or credit cards.

It works like this: a thief gets his hands on a supply of key cards, either by having a hotel employee steal a batch or by buying them. The thief then uses a commercially available decoder/encoder to read information off a stolen credit card and transfer it to an innocent-looking hotel key card. Because the new generation of key cards is the same size as credit and debit cards, the key cards can then be used at ATMs and at point-of-sale swipe readers, where store clerks frequently do not watch patrons performing the transactions.

The scam recently came to light in southern California when police searched the hideouts of Armenian gang members and found a cache of key cards from a specific hotel. According to Larry Hanna, a detective in the Las Vegas Police Department's intelligence unit who works closely with Southern California police, authorities decided to read what was encoded on the cards. They came up with credit, ATM, and debit card numbers, but no room information.

Blair Abbott, a Phoenix-area detective who has been investigating this type of crime, notes that a few key cards found on a suspect will not raise the same suspicion as would several credit cards bearing different names. Having multiple hotel keys is neither illegal nor uncommon.

Abbott also believes that the scheme is causing a resurgence in the use of readers that steal information from bank and credit cards at ATM machines. His firm investigated a criminal group that devised a credit card reader that could be placed over the normal credit card slot in ATMs and other card readers. The device has all the appearances of a regular card reader, but it is distinguished by protruding from the face of the ATM by several inches. Abbott adds that clever criminals have even created their own bogus ATM machines.

When the card information is lifted and placed on hotel key cards, it can be used not only at point of sale and at ATMs but also in association with accomplices working at stores, banks, and credit card companies. Worse yet, the victim continues to use his or her credit card and will attest to having it when contacted by the credit card company, which delays detection of the fraud.

Law enforcement has had to rely on the laziness of criminals to spot the scheme, Abbott says. Carrying several cards from the same hotel arouses suspicion, says Abbott, as does punching holes in cards and attaching them to a key chain.

It is unclear how widespread the scam is, but Hanna points out that it is so well known in Glendale, California, that the police keep a reader at the booking desk to scan all confiscated hotel key cards. Abbott says that the ploy is making the rounds in New York and Chicago as well.

However, this scheme doesn't depend upon harvesting personal information by reading it from returned hotel key cards; it's based upon criminals' obtaining personal information (such as credit card or ATM card numbers and PINs) through other methods and then using discarded hotel key cards as storage media for that information. Loyalty cards issued by grocery stores (used to gain information about which products are selling at which locations to which groups of customers) or slot club cards issued by casinos (used to track the play of gamblers) could just as easily be used for this purpose.

Nonetheless, those who remain concerned that they may be discarding sensitive personal information with their hotel keys can follow the piece of advice offered in the message quoted at the head of this page: When you check out of your hotel, simply retain or destroy your keycard. Your former room's access code will be changed before the room is assigned to a new guest, and few (if any) hotels demand that keycards be returned or charge customers who fail to do so. Just be sure that you are the one who retains or destroys the card.

Additional information:



Hotel Key Card Update
(Pasadena Police Dept.)



It's Just the Key to Your Room
(Computerworld)



Local Hotels Debunk Keycard ID Theft Risk
(bend.com)

Last updated: 9 June 2010

The URL for this page is <http://www.snopes.com/crime/warnings/hotelkey.asp>

Urban Legends Reference Pages © 1995-2010 by Barbara and David P. Mikkelson.
This material may not be reproduced without permission.
snopes and the snopes.com logo are registered service marks of snopes.com.



Sources:

Casper, Stacey. "Warning: Your Room Key May Not Be Safe."
Good Housekeeping. November 2004 (p. 79).

Le, Phuong Cat. "Reversed PIN Isn't a 911 Call, Hotel Key Cards Keep Mum."
Seattle Post-Intelligencer. 30 January 2007.

Lerten, Barney. "Local Hotels Debunk Keycard ID Theft Risk."
Bend.com. 17 October 2003.

Mitchell, Robert. "It's Just the Key to Your Room."
Computerworld. 16 January 2006.

Morrison, Jane Ann. "Hotels Can't Erase Myth About Credit Card Information on Room Keys."
Las Vegas Review-Journal 10 November 2003.

[Is Your Bank In Trouble?](#)

Free list Of Banks Doomed To Fail. The Banks and Brokers X List. Free!

www.MoneyAndMarkets.com