

GlobalTM travel products

Wireless identity theft - From Wikipedia, the free encyclopedia

Wireless identity theft, also known as **contactless identity theft** or **RFID identity theft**, is a form of identity theft described as "the act of compromising an individual's personal identifying information using wireless (radio frequency) mechanics."^[1] Numerous articles have been written about wireless identity theft and broadcast television has produced several investigations of this phenomenon.^{[2][3][4]} According to [Marc Rotenberg](#) of the [Electronic Privacy Information Center](#), wireless identity theft is "a pretty serious issue" and "the contactless (wireless) card design is inherently flawed".^[5]

Efforts are currently under way to educate consumers as to the vagaries of [Radio Frequency Identification \(RFID\)](#) which can pose a threat, as well as attempting to initiate legislation to limit the use of RFID technology by companies and governmental agencies.^[citation needed]

[\[edit\]](#) Overview

Wireless identity theft is a relatively new technique of gathering an individual's personal information from RF-enabled cards carried on a person in their [access control](#), credit, debit, or government issued identification cards.^[6] Each of these cards carry a Radio frequency identification chip which responds to certain radio frequencies. When these "tags" come into contact with radio waves, they respond with a slightly altered signal. The response can contain encoded personal identifying information, including the card holder's name, address, Social Security Number, phone number, and pertinent account or employee information.

Upon capturing (or 'harvesting') this data, the thief is then able to program their own cards to respond in an identical fashion (via 'cloning'). Many sites are dedicated to nothing but teaching people how to perform this act, as well as supplying the necessary equipment and software.^{[7][8]}

The financial industrial complex is currently migrating from the use of magnetic stripes on debit and credit cards which technically require a swipe through a magnetic card swipe reader. These transactions take approximately 48 seconds, whereas the newer radio frequency tagged card transactions require approximately 12 seconds.^[citation needed] The number of transactions per minute can be increased, and more transactions can be processed in a shorter time, therefore making for arguably shorter lines at the cashier.^[9]

[\[edit\]](#) Controversies

Academic researchers and ['White-Hat' hackers](#) have analysed and documented the covert theft of [RFID](#) credit card information and been met with both denials and criticisms from RFID card-issuing agencies.^{[11][10]} Never-the-less, after public disclosure of information that could be stolen by low-cost jury-rigged detectors which were used to scan cards in mailing envelopes (and in other studies also even via drive-by data attacks), the design of security features on various cards was upgraded to remove card owners' names and other data.^{[11][10]} Additionally a number of completely unencrypted card designs were converted to encrypted data systems.^{[11][10]}

[\[edit\]](#) RSA Report

The issues raised in a 2006 report were of importance due to the tens of millions of cards that have already been issued.^{[11][10]} [Credit](#) and [debit card](#) data could be stolen via special low cost radio scanners without the cards being physically touched or removed from their owners' pockets, purses or carry bags.^{[11][10]} Among the findings of the 2006 research study, "Vulnerabilities in First-Generation RFID-Enabled Credit Cards", and in reports by other white-hat hackers:

- some scanned credit cards revealed their owners' names, card numbers and expiration dates;^{[11][10]}
- that the short maximum scanning distance of the cards and tags (normally measured in inches or centimetres) could be extended to several feet via illicit technological modifications;^{[11][10]}
- that even without range-extension technologies, [Black Hatters](#) walking through crowded venues or delivering fliers could easily capture card data from other individuals and from mail envelopes;^{[11][10]}

Global Travel Products 17/49 Corporate Blvd, Bayswater Vic 3153 - PO Box 1044, Bayswater Vic 3153

Ph: 03 9721 8020 Fax: 03 9721 8021 ABN: 93268095155

www.globaltravelproducts.com.au E-mail: info@globaltravelproducts.com.au

Logical Distribution Pty.Ltd trading as Global Travel Products ABN: 93268095155

GlobalTM travel products

- that security experts who reviewed the study findings were startled by the breaches of privacy of the study (conducted in 2006);^{[1][10]}
- that other e-systems, such as [Exxon Mobil's Speedpass](#) keychain payment device, used weak encryption methods which could be compromised by a half hour or so of computing time;^{[1][10]}
- that some cards' scanned stolen data quickly yielded actual credit card numbers and didn't use data tokens;^{[1][10]}
- that data illicitly obtained from some cards was successfully used to trick a regular commercial card-reader (used by the study group) into accepting purchase transactions from an online store that didn't require the entry of the cards' validation codes;^{[1][10]}
- that while higher level security systems have been and continue to be developed, and are available for RFID credit cards, it is only the actual banks which decide how much security they want to deploy for their cardholders;^{[1][10]}
- that *every one* of the 20 cards tested in the study was defeated by at least one of the attacks the researchers deployed;^{[1][10]}
- another related security threat concerned a different product: new government issued [ePassports](#) ([passports](#) that now incorporate RFID tags similar to credit and debit cards). The RFID tags in ePassports are also subject to data theft and cloning attacks.^[1] The [United States government](#) has been issuing ePassports since [2006](#).^{[5][10][11]}

In a related issue, privacy groups and individuals have also raised [Big Brother](#) concerns, where there is a threat to individuals from their aggregated information and even tracking of their movements by either card issuing agencies, other third party entities, and even by governments.^[12] Industry observers have stated that: '*...RFID certainly has the potential to be the most invasive consumer technology ever*'.^[12]

Credit card issuing agencies have issued denial statements regarding wireless identity theft or fraud and provided marketing information that either directly criticized or implied that:

- beyond the card data itself, other data protection and anti-fraud measures in their payment systems are in place to protect consumers;^[10]
- the academic study conducted in 2006 used a sample of only 20 RFID cards, and was not accurately representative of the general RFID marketplace which generally used higher security than the tested cards;^[10]
- unencrypted plain text information on the cards was "...basically useless" (by itself), since financial transactions they were tied to used verifications systems with powerful encryption technologies;^[10]
- even if consumers were victims of RFID credit card fraud or identity theft, they would not be *financially* liable for such credit card fraud^[10] (a marketing strategy that ignores the other serious consequences to card holders after they've been associated with fraudulent transactions or have their [identity stolen](#));

After the release of the study results, all of the credit card companies contacted during the [New York Times'](#) investigative report said that they were removing card holder names from the data being transmitted with their new second generation RFID cards.^{[5][10]}

As of December 2008, it is estimated there are at least 270 million RF tagged contactless debit and credit cards in circulation in the North America.^[citation needed]

[\[edit\]](#) Compromised U.S. identification documents

Certain official identification documents issued by the U.S. government, [U.S. Passports](#), Passport Cards, and also enhanced driver's licenses issued by States of New York and Washington, contain RFID chips for the purpose of assisting those crossing the U.S. border.^[13] Various security issues have been identified with their use, including the ability of [black hats](#) to harvest their identifier numbers at a distance and apply them to blank counterfeit documents and cards, thus assuming those people's identifiers.^[13]

Various issues and potential issues with their use have been identified, including privacy concerns. Although the RFID identifier number associated with each document is not supposed to include personal identification information, "...numbers evolve over time, and uses evolve over time, and eventually these things can reveal more information than we initially expect"

GlobalTM travel products

stated Tadayoshi Kohno, an assistant professor of computer science at [University of Washington](#) who participated in a study of such government issued documents.^[13]

[\[edit\]](#) MythBusters

[Adam Savage](#) of the science TV show [MythBusters](#) stated during the July 2008 HOPE conference in New York City, that when they were going to demonstrate how RFID worked and their vulnerabilities in financial exchange cards, their lawyers were challenged by other lawyers representing RFID vendors and several banking institutions. It was made verbally clear to the Mythbusters team that advertising for their show would be pulled by the finance industry if any demonstration of contactless card vulnerabilities was conducted.{{L}}

[\[edit\]](#) See also

- [Identity theft](#)
- [RFID](#)
- [HID Global](#)
- [Credit card fraud](#)

[\[edit\]](#) References



This article relies on [references to primary sources](#) or **sources affiliated with the subject**, rather than references from independent authors and third-party publications. Please add [citations](#) from [reliable sources](#). (May 2009)

1. [^][a b c d e f g h i j k l m n o p](#) Heydt-Benjamin, Thomas S; Bailey, Daniel V; Fu, Keven E; Juels, Ari & O'Hare, Tom [Vulnerabilities in First-Generation RFID-enabled Credit Cards](#)^[*dead link*], University of Massachusetts, Amherst, MA; RSA Laboratories, Bedford, MA; Innealta, Inc. Salem, MA; Innealta.com, draft study dated October 22, 2006, retrieved 2009-03-14; A copy of the document can be obtained at [Vulnerabilities in First-Generation RFID-enabled Credit Cards](#)
2. [^] Annalee Newitz, Annalee (2006) [The RFID Hacking Underground](#) <http://www.wired.com/wired/archive/14.05/rfid.html> Wired.com, May 2006 Vol. 14.05
3. [^] [KPHO-5 PHOENIX website](#);
4. [^] [KVUE-24 Austin website](#);
5. [^][a b c](#) Weston, Liz Pulliam (2007) [New Credit Cards Allow Hands-Free Theft](#), MSN Money website, 2007-12-21, retrieved 2009-03-14;
6. [^] [Position Statement on the Use of RFID on Consumer Products](#) Electronic Freedom Foundation website
7. [^] [RFIdiot website](#);
8. [^] [Texas Instruments' RFID website](#);
9. [^] http://usa.visa.com/personal/cards/paywave/micro_tag.html
10. [^][a b c d e f g h i j k l m n o p q r s t](#) Schwartz, John (2006) [Researchers See Privacy Pitfalls in No-Swipe Credit Cards](#), New York Times, 2006-10-23
11. [^] [Are New Passports Identity-Theft Risk?](#) WorldNetDaily.com, October 21, 2004;
12. [^][a b](#) Booth-Thomas, Cathy; Barnes, Steve; Cray, Dan; Estulin, Chaim; Israely, Jeff; Mustafa, Nadia; Schwartz, David and Thornburgh, Nathan (2003) [The See-It-All Chip](#) Time Magazine, September 22, 2003;
13. [^][a b c](#) Naone, Erica [Identification: RFID's Security Problem: Are U.S. passport cards and new state driver's licenses with RFID truly secure?](#), [Technology Review](#) by [M.I.T.](#), January/February 2009, pp.72-74 (subscription).

[