# RFIDprotect SM

case studies 2011

www.rfidprotect.co.uk

# Case Study # 7:
# US Deptartment of Defense - tool up!

The year 2011 will surely mark a significant turning point in the debate surrounding 'contactless' credit, debit, passport and door-access security. For as 2010 drew to a close, Secure ID News broke the following news,

*"…2.5 million radio frequency shielding sleeves (were delivered) to the Department of Defense to protect the contactless Common Access Card (CAC) from data interception. The FIPS 201-approved, shielding sleeves are distributed via RAPIDS ID offices worldwide with the issuance of new CACs."*

The online journal then went on to explain that an additional order for *1,675,000* shielding sleeves had been placed by the Defense Department for delivery in January 2011. RFID Protect has also learned that this investment in *'anti-skimming'* technology brings the total number of units issued to the US military to approximately 4.2 million.

Of course, whilst unauthorised data interception from RFID enabled devices is not common – this development would strongly suggest that the potential threat of *'skimming'* is a real issue for the security services, and a matter that is now given the most careful consideration.

Author: This short case study references an original publication by Secure ID News

Original source: http://www.secureidnews.com/2010/11/29/defense-department-order-rf-shields-from-national-laminating
Date: 29 November 2010

RFIDprotect™

www.rfidprotect.co.uk

# Case Study # 8:

## Ski passes – easily skimmed and cloned

If you've been issued with a new RFID enabled, or 'contactless' ski pass then there's a risk that it may be intercepted, read or skimmed, and without your knowledge. A new generation of ski and lift passes are already being rolled out across US and European resorts, and you may not realise that contained within them is a small passive RFID microchip. This bit of clever kit enables swift access to the slopes, and other services off-piste.

Great news! But not so great news if you don't want marketers to track your every movement, and transaction, whilst on holiday.

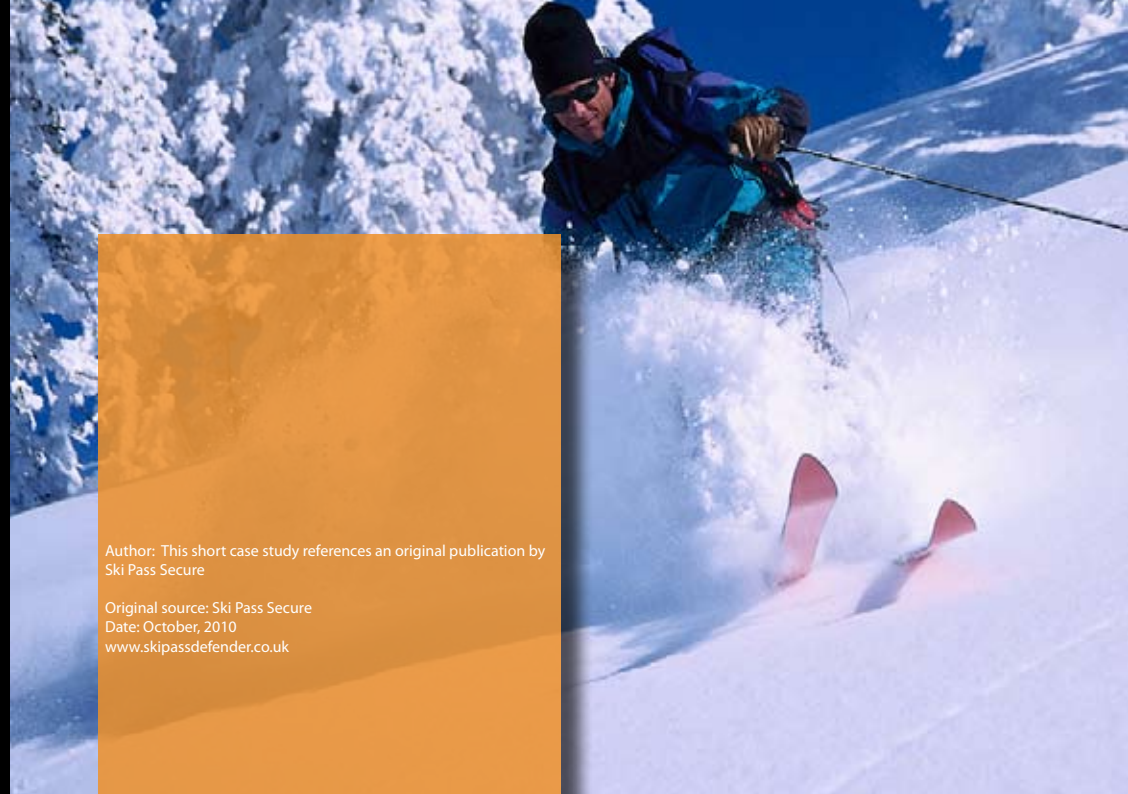
Furthermore, it's well documented that unscrupulous hackers have been able to skim these 'contactless' passes using low-cost readers freely available on line. The consequences can be that your personal information and movements can be tracked and exploited for commercial or criminal gain.

We're passionate about snow! And we care about anything that could ruin your day on the slopes. When we discovered that newly issued 'contactless' ski-passes could be hacked, skimmed or used in covert market research then this was something that we felt others ought to be aware of.

RFID Protect can now supply 13.56MHz RFID enabled ID card / ski-pass holders designed to protect RFID enabled ID and door entry cards from being skimmed.

RFIDprotect™

www.rfidprotect.co.uk



Author: This short case study references an original publication by Ski Pass Secure

Original source: Ski Pass Secure
Date: October, 2010
www.skipassdefender.co.uk

# Case Study # 9:
# Misuse of RFID technology…

A stark warning from the European Union Consumer group (BEUC) suggests that unless legislation is brought in to control the use of RFID based technology, the clothes that we wear could end up giving away more about the wearer than they would perhaps like.

BEUC points to a fashion store chain in Germany, which is pioneering a scheme using clothes tagged with RFID chips. The project links images of accessories, (which are displayed on a screen inside the shop changing room), whenever a customer takes in any RFID-tagged clothing. Thus creating the potential for a perfect ensemble, and more importantly for the retailer it encourages further purchases. Driving additional sales in isolation is a perfectly reasonable practice.

However a major concern, (which was raised by the BEUC), is the method used to disable these RFID chips once customers have made their purchase and left the store. Often the RFID device is not disabled!

RFID tags/chips can be linked with a customers' payment card (credit or debit card) at the point-of-sale, along with other personal data; including their buying habits. This leaves the very real possibility of data profiling by retailers and criminals.

Emilie Berrauin - in an interview with Tech Radar in 2008 - suggested that unless the development of RFID technology is subject to EU law early on, then future repercussions could be massive.

RFIDprotect™

www.rfidprotect.co.uk

Emilie Berrauin says, *"...RFID technology is not widely developed, but in five years it could be widespread. As each chip functions as a unique identifier, it can be linked with personal data and is able to be read by anyone with a suitable reading device. We firmly believe that there is potential for misuse and they should be deactivated at the point of sale."*

The EU retail industry is looking to implement a voluntary *'opt-out'* scheme, where the customer is responsible for ensuring RFID chips are deactivated before leaving the store. BEUC prefers an *'opt-in'* approach.

Author: Tech Radar | *Concern over misuse of RFID chips* | By Audley Jarvis | March 3rd 2008

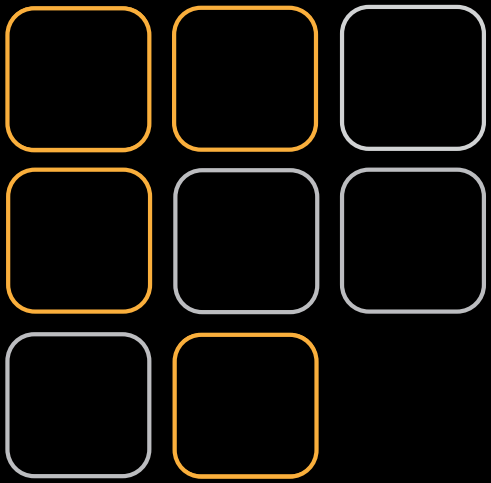
Original source: http://www.techradar.com/news/world-of-tech/future-tech/concern-over-misuse-of-rfid-chips-255699#ixzz16tWs5vTG

# Contacting us

Business hours are 9:30am to 5:30pm GMT

For further information:

T: +44 01234 772632
E: sales@rfidprotect.co.uk





RFIDprotect™


RFIDprotect℠