



14 Bentinck Court, Bentinck Road, West Drayton,
Middx, England. UB7 7RQ.

www.storm-interface.com

Storm Interface is a trading name of Keymat Technology Ltd.

Who's In Your Wallet?

We face a real and present threat to our national security. This threat originates from both domestic and foreign sources. As an increasing number of countries move to adopt secure credit card transaction technology, eastern European cartels are turning their attention to the relatively unprotected US card transaction system. However more sinister organisations may already be at work.

International intelligence sources report that money obtained through credit card fraud has been used to fund terrorist organizations. When, in December 2000, police agencies intercepted an attempt to bomb the Christmas Market in Strasbourg France, they uncovered an al-Qaeda cell operating across international borders. During subsequent interrogations and investigations it was discovered that the cell's activities had been financed by the use of cloned credit cards. These activities included the purchase of bomb making materials for use in the Strasbourg attack. Several cloned cards were recovered during raids on apartments and houses used by cell members in Frankfurt Germany and London England. The arrest and conviction of two suspected Algerian terrorists by UK authorities is thought to be indicative of more widespread use of credit card fraud by extremist organizations.

Crimes involving credit card cloning and identity theft are growing in scope and frequency. In the USA a fraudulent card transaction is completed every 8 seconds. According to the Federal Trade Commission, identity theft accounts for 42% of complaints registered by consumers. With U.S. intelligence agencies in possession of this information, surely the declared 'War on Terrorism' could be most effectively waged by denying illegal organizations the oxygen of funds; especially funds stolen from U.S. citizens and corporations. This is not a matter of whether losses through fraud are sustainable by the financial institutions, it is a matter of morality and national security. Losses resulting from fraud are ultimately reflected in the interest payments levied on credit card users. American consumers are unknowingly financing terrorist activities. Why then do U.S. authorities appear to be so slow in responding to this avalanche of fraud?

In Britain retailers have been 'encouraged' to invest in a new 'secure' transaction technology by a shift in responsibility for fraudulent transactions. The credit card companies simply changed the rules! They mandated that if retailers failed to adopt a more secure 'chip and PIN' technology the retailer would bear an increased responsibility for the losses caused by fraud. The banks and the card companies would no longer pick up their share of the tab. Unsurprisingly, most retailers could not insure against the risk, nor could they bear the potential losses. The net result was a dash to install new and more secure payment terminals before the deadlines kicked in. By the end of this year British

consumers will not be able to use their credit cards without keying in a four digit 'Personal Identification Number' (PIN). The credit card they 'insert' (note; insert not swipe) will need to have a secure embedded micro-processor (chip) carrying details of their identity and transaction status. This new 'chip and PIN' system dispenses with subjective (and notoriously unreliable) signature checking. The new credit and debit card terminals also include sophisticated fraud detection and protection systems at hardware, firmware and software levels. Any attempt by fraudsters to tamper with the system, at any level, will trigger the protection measures. Precise details of how these measures work are withheld for obvious reasons.

This 'Chip and Pin' card technology is in stark contrast to the U.S. transaction system which requires only possession of the credit card (or a copy of it). The new European system requires possession plus knowledge. To make any transaction you need possession of the card and knowledge of the PIN. Without both these things all transactions will be refused. No worries if you accidentally leave your card in a gas station. Without your PIN the card is useless. Industry analysts predict that in the future, possession, plus knowledge, plus attribute may be required to ensure ultimate levels of security. An attribute is a characteristic unique to you as an individual. It may be a finger-print, a palm print, a retina pattern or even a thermal map of your head. All these bio-metric recognition technologies exist now. They are commercially available.

The Federal Trade Commission rates 'identity theft' as one of American consumer's top three concerns. Are we right to be concerned? Let's consider what happens when we visit the gas station to fill up, a transaction completed by millions of Americans each and every day. As we swipe our card through the pump's magnetic stripe reader (MSR) does anyone check for a signature, or even ask our name? No! Okay, but before the bad guys can start filling their cars (or trucks) at our expense they are going to need a copy of our card. How could they get that?

It's easy! Many reputable electronic component distributors will sell you a card reader. Some so small you could hide one in the palm of your hand. Every time we hand our credit card to a sales assistant or restaurant waiter we run the risk of 'card skimming'. You don't even have to hand the card over! Merely swiping your own card at the gas pump exposes you to the risk of card cloning. If the 'bad guys' can open the gas pump's control panel they can install a miniature reader (referred to as a bug) which copies the data from the magnetic stripe on your card. A clone of your card can be made within seconds! This may sound like science fiction, but the truth is it happens every day! Bugs have been found in gas pumps, vending machines, ATMs, public internet terminals, car wash program selectors and ticketing machines. The more responsible equipment manufacturers have already recognized the problem and are moving to secure their machines against unauthorized access; but there are currently millions of insecure installations spread across the continental U.S.

It seems too obvious to say that we must improve the security of our transaction infrastructure, but without the adoption or (dare I say) federal mandating of new standards for credit card technology there is a danger that the American public will lose confidence. We should be able to use our cards without wondering "who's in our wallet". Confidence in the security of our financial systems is essential not only for our economy but also our national security. Will we be seeing a new generation of 'street wise' transaction terminals here in the USA? Let's hope so!

The initial breakthrough came over Christmas 2000 when the German equivalent of the SAS burst in on a flat in Frankfurt. They arrested four men and uncovered an arsenal with bomb-making chemicals, weapons, cloned credit cards and false documents.

Extract from BBC News "The secret war against al-Qaeda" broadcast 10th Feb 04.