



PROXIMAL CONSULTING

www.proximalconsulting.com

ATM Fraud: Unjustified Panic or Real Problem?

In July 2004 First Direct did something very strange: it wrote to its customers and asked them to use cash machines as little as possible. Why did it write to 110,000 customers with this advice? Because First Direct believed that "making frequent withdrawals from ATMs increases your exposure to fraud". This morning I went to a cash machine to withdraw some cash – and the first thing that I noticed was the large poster advising me that if the ATM doesn't look like the photograph shown then I should not use it as it has been tampered with.

So are these warnings a sign of unjustified panic – or is there a real problem? Cashpoint fraud is reported as costing £39 million each year – although this figure, like all such estimates – is probably an underestimate rather than the opposite. The world's ATM (CashDispenser) networks are a prime example of how small the world has become in the digital age. But it should be borne in mind that this is very much old technology.

You are now able to use your plastic card at virtually any ATM across the world. The technology of ATM cards and machines is in essence very simple - your ATM card has a magnetic stripe, which contains your account number and perhaps some information about the card issuer. You insert your card into an ATM and key in your PIN (Personal Identification Number) - that is then relayed through telecommunications links back to your card issuer's home computer, which checks your account number, compares the PIN you have keyed in against the one it holds for you ("user authentication") and then validates that you have the money in your account that you have requested to withdraw (or an overdraft to cover it). All of this takes place in a few seconds. Even though the ATM that you are using is in Singapore and your card issuers computer is in Madrid. The big draw for criminals is that cash withdrawn from ATMs all across the world is in the region of \$1 trillion annually.

Banks have for years urged customers not to keep their plastic cards and PIN numbers together. However there is of course one place where it is impossible not to have the card and PIN number together...and that's when you are withdrawing from a cash dispenser, and that's where these criminals are most active. One simple and very common fraud at cash dispensers is where the person behind you in the ATM queue peers over your shoulder and memorizes your PIN as you key it in (or uses a cheap video camera or web cam to capture the details of your PIN) – this technique has now been dubbed "shoulder surfing". You wait for the card to be returned by the machine, but before that happens an attractive young lady taps you on the shoulder to tell you that you have dropped some money on the floor. Miraculously (particularly if the reason you went to the ATM was because you had no money) there is a £10 note on the floor, which you pick up. Whilst you are doing that, the gentleman behind you has quickly pocketed your card as it is returned by the ATM. You are left to presume that the ATM has "swallowed" your card, but want to leave the scene quickly because you are £10 richer. By the time you phone the card issuer to report that the machine has "swallowed" your card it has been used to its limit in numerous ATMs - and if it is a credit or debit card probably in a few shops as well.

The other most common cash dispenser fraud has become known as the "Lebanese loop" because criminals of Lebanese origin apparently first used it. This has many variations but usually involves the cash machine being tampered with so that your card is not returned to you and is then removed by the criminals: alternatively if you get your card back a device has recorded the details of your magnetic stripe. The crooks have also captured your PIN number though some variation of shoulder surfing. It is this problem that has led to banks putting posters and other warnings on ATMs advising customers to visually inspect the machine to see if it has been altered or tampered with.



PROXIMAL CONSULTING

www.proximalconsulting.com

Whilst my experience is that ATM crime has been in existence for at least fifteen years, and has been perpetrated by all types of criminal – from opportunistic to highly organised groups a possible and very worrying new trend has emerged. In December 2004 Jean-Louis Bruguiere, the top French anti-terrorism judge, claimed that radical terrorist cells in Europe are generating hundreds of thousands of pounds each month to finance their activities through cash machine scams, mostly using variants of the Lebanese loop.

And of course, if you are the victim of ATM fraud, your money has been stolen. So whilst I don't suggest not using cash dispensers, I think it is best to be careful and observant when you do use them.

Peter Lilley is the head of Proximal Consulting, a business crime prevention firm. He is also the author of various books including "Hacked, Attacked & Abused: Digital Crime Exposed".

This article was originally published in the March 2006 edition of Asian Voice