BANKS are facing a crisis of public confidence in ATMs as a result of security failures, NCR fraud specialist Claire Shufflebotham says. "Yes, people like the convenience of ATMs, but banks have encouraged their use as a means of reducing overall costs," she says.

"It would be a nightmare if consumers were to lose confidence in self-service and flock back to the branches."

Shufflebotham, of NCR's ATM offices in Dundee, Scotland, says fraud, scams and software failures have raised "unhelpful" concerns about ATM-user safety and security.

The financial sector had traditionally been secretive about fraud, "but secrecy doesn't help", she says.

"If we want consumers to continue to trust and use ATMs, we have to be more proactive. Let's not wait for the next attack, let's put measures in place across the cash chain to minimise the risk at the ATM."

Australian Bankers' Association chief executive David Bell says banks are constantly reviewing security, including customer safety at ATMs.

"Crime prevention is a key consideration in siting bank ATMs," he says.

"ATMs are usually located in well-lit areas that are highly visible to passing traffic and free of obstructions.

"Robberies at ATMs are rare, but wherever there is cash it pays to be careful. If at any time you don't feel comfortable, we suggest using Eftpos to withdraw cash at supermarkets and service stations."

Shufflebotham says ATM crime is no longer the domain of amateurs or a spur-of-the-moment offence.

International, organised gangs are targeting any weak link — either electronic or physical — in banking systems worldwide.
Banks no longer keep their cash in a vault, but in thousands of ATMs in thousands of corner stores.

Australians withdrew more than $115 billion in cash from ATMs in 2002, according to Reserve Bank estimates.

That kind of cash is bound to attract thieves, and it has led to new crimes such as card trapping, skimming and identity theft.

"Criminals are inventive," Shufflebotham says. "Of course there are physical attacks, on cash-in-transit employees or in ram raids, where the contents of a machine are simply loaded on to a truck. The potential for theft through fraud is also huge."

So far, the main crimes have involved capturing the card (trapping) or illegally copying the data in the card's magnetic strip (skimming).

Shufflebotham says skimming is far worse because people are unaware their card has been skimmed.

"If a thief rigs an ATM so that a card is trapped, the customer walks away thinking the machine has eaten their card, and will contact the bank," she says.

"If there's a skimming device somewhere, however, the victim won't have a clue. This is where we are seeing huge growth in ATM-related fraud."

Australian consumers are particularly at risk because local banks have been slow to adopt more secure chip-card systems, she says.

Law-enforcement agencies have noted gangs shifting their operations from countries such as Malaysia, Thailand, Taiwan and Singapore — where smart cards have been mandated — to softer targets still using mag-stripe cards.

This trend has been confirmed by the Australian Crime Commission, which says skimming was the fastest growing scam last year, accounting for 50 per cent of all credit-card fraud (up from 5 per cent two years ago).

Skimming gangs ripped off $100 million from unsuspecting citizens last year, according to the ACC.

The Federal Government has responded with a flurry of announcements: task forces on fraud and identity theft, special intelligence operations, a national skimming database, new laws and education campaigns.
The ABA’s Bell says Australian banks receive intelligence from overseas sources, including alerts about new devices and tricks used by criminals.

"The banking industry has just launched a major campaign to help businesses tackle credit-card fraud and skimming," Bell says. "This will be rolled out to tens of thousands of merchants over the next month."

Individual banks also have their own fraud detection tools and strategies, and they are always looking at new offerings from suppliers, he says.

The familiar landscape is changing, though. Yes, Australians have embraced banking technologies — according to the Australian Payments Clearing Association there are about 21,000 ATMs and 430,000 Eftpos terminals nationwide.

But greater availability for customers means more opportunities for criminals.

For a start, there’s the emergence of non-bank providers or "white brand" ATMs that are increasingly being put in open areas such as petrol station forecourts and shopping malls.

This trend poses new risks for cash-in-transit security staff, merchants and customers.

"More cash is being moved across the pavement than ever before," says Ray Lambie, chief executive of security company Corporate Protection Services.

Guards have to venture further from their armoured vehicles to keep ATMs cashed up, increasing the risk of physical attack on personnel.

Shop owners also face more attacks.

In recent months, a Sydney "cash-and-carry gang" netted more than $100,000 in a string of ram raids and in four instances teams of thieves hauled an ATM out of a shop window and escaped in a stolen vehicle.

Nevertheless, ATM Industry Association executive director Jon Andreasson says the number of ATMs worldwide will continue to grow — from 1.1 million today to 1.7 million by 2007.

Most of the new machines will be away from bank premises, he says.

Australia will follow the lead of the US, where 62 per cent of ATMs are in service
stations, malls and convenience stores, compared with about 25 per cent here.

Andreasson says stealing card data through skimming, trapping and phishing — where consumers respond to fake emails that appear to be from legitimate banks and financial institutions — is a greater long-term risk.

Phishing is growing at frightening speed, he says.

In January, 176 new phishing attacks were reported in Australia, up 52 per cent from a month earlier.

Andreasson says fraud related to identity theft cost about $US33 billion ($45 billion) worldwide last year, and US data suggests each instance cost victims an average $US10,000, and took up to 60 hours to sort out. He says identity theft is an extremely complex crime.

"The victim is generally considered guilty until proven innocent," he says.

NCR’s Shufflebotham says financial institutions will have to do more to protect customer data and employee safety at ATMs.

Physical measures include products intended to foil trappers and skimmers — see-through surrounds for card readers, a "jitter" device that prevents a clean read of mag-stripe data, and triple-DES encryption on the keyboard to protect PINs.

NCR is promoting an ink-dye banknote destruction system, similar to dye-tags that ruin a garment when a shoplifter tries to remove it.

Cassettes of purple ink explode over the cash and the thief when a machine is attacked.

Although ink degradation is yet to be used in Australia, British company Travelex has deployed about 500 ink-dye ATMs across Europe.

"This is all about spoiling the prize, so it isn't worth going after the hard cash," Shufflebotham says.

"There's also a version for cash handlers — the risk to them should be greatly reduced, so if someone illegally opens the cassette the banknotes are rendered worthless."

But in the longer term, she says, internet worms and viruses pose a huge new threat to ATM networks that run on embedded
software of popular operating platforms such as Windows XP.

ATMs are among a range of devices, including emergency response and in-car systems, unexpectedly vulnerable to attack over the internet.

Several incidents over the past year have shown that even machines supposedly isolated from the internet are vulnerable.

"Software security is the biggest risk to ATMs right now," Shufflebotham says.

The industry has been shaken by recent attacks that hit cash machines produced by a rival US manufacturer, Diebold.

In the worst incident, the Bank of America's network of 13,000 Diebold ATMs was knocked out for a day in October by Nachi, a variant of the MSBlaster worm.

The same network had been forced down in January 2003 when the Slammer worm created so much traffic that transactions could not be processed.

Shufflebotham says the Nachi outage cost the bank millions, and "raised questions" about the integrity of the underlying Windows XP-embedded software.

US researchers say Nachi spread through a flaw in Windows XP, 2000, NT and Server 2003, causing major disruption to corporate networks.

The worm may have reached the ATM network through an undocumented connection to the internet, or it may have been inadvertently spread beyond the firewall by a laptop.

In yet another extraordinary breach, Shufflebotham says students at Carnegie Mellon University in Pittsburgh crashed a Diebold ATM last month by unplugging it and were amazed to discover the machine rebooted as a Windows XP desktop.

Because there was no user ID or password protection, the students were able to use it to access music and other programs.

This report appears on australianIT.com.au.