Prevention of Cheque Fraud

Dr Chris Crozier, Cirrus Techvue
Tel.: +27 11 783 1508 email: chris@cirrus.co.za

I used to say that prevention of cheque fraud is not a simple matter. In fact, generally it is; but it is not an *easy* matter. It is a battle that has to be fought on many fronts. Overlooking one or two points of vulnerability is as good as having a boat that only leaks in a couple of places, with any of the holes having the potential to grow catastrophically without notice.

I remember having a discussion with a friend some time ago about the ability of a mosquito to find the smallest tear in a mosquito net. He wanted to attribute it to some special ability of the mosquito that defied our understanding. I hold a much more mundane view. To my mind, all the mosquito has going for it is an enormous persistence. It is quite prepared to spend the whole night knocking its head repeatedly against the net until at last it finds a way through. Of course, the other advantage the mosquito has is that it is one of many. There may be a hundred mosquitoes trying to get through your net: if only one succeeds then you think that the mosquito has won the battle. From the point of view of individual mosquitoes this is a moot point. From your perspective, however, there is no doubt that you have lost.

Dealing with cheque fraud is in many ways similar. There are a great number of potential criminals out there, and many fronts on which they can attack you. Most of them will fail, but the important point for you is that if only one of them succeeds, you have lost.

Your defence against cheque fraud must be based on the presumption that any chink in your armour will be discovered. You must, therefore, look at all aspects of cheque issuing, from the initial printing of the cheques, through the issuing of them, and even to the safe-keeping of them once the processed cheques have been returned to you.

Cheque Fraud 101: A Primer

Let's look at what you need to perpetrate a cheque fraud.

1. You need to steal a cheque. That is seldom hard, and can be remarkably easy. There are so many ways for it to be done that you must assume that it can happen.
2. You need a fraudulent account. Opening an account is far too simple. When cheque fraud is costing the country millions upon millions every year, it seems inappropriate for banks to compete on how quick and easy it is to open an account – you can even do the whole transaction by phone. False ID books sell for around R200. So now the thief has an account waiting to receive the stolen funds.
3. You need to be able to pay the cheque into the account. A cheque is made out to a specific payee. The thief's choices are to masquerade as the matching payee, or to alter the payee name to suit the account.

   The first option can be tricky, particularly as they don't often know in advance the payee that will be on the cheque, and in many cases attempting to open an account in the name of the intended payee may raise suspicions; so it is far commoner to adjust the payee name.

   And while they are busy anyway, if the cheque is a bit small, they may well want to do something about making all that effort a bit more worthwhile. This is the stage where the crooks can get a lot of help from you, the cheque issuers. Remember that a lot of actual and potential criminals out there are quite prepared to spend hours on end, even days, doing painstaking, tedious work. People who are willing and able to change their lives, move to new homes, for a few tens of thousands of Rand.

Risk Assessment

Risk assessment is unfortunately not an exact science. Statistical data is hard to come by and rarely reliable, so all too often we must fall back on gut feel. Our perception of the severity of a

particular risk is strongly affected by our own experiences and knowledge. Knowing exactly how to perpetrate a particular form of fraud can influence us both ways: you might see something as relatively easy to do, and therefore representing a high risk, when in fact the number of people with the necessary knowledge and skills to carry out the actions might be few and far between; on the other hand, not knowing too much about something might lead you to presume it to be a lot harder to do then is in fact the case. It doesn't help that you will get conflicting advice from sources that are seldom unbiased.

You can categorise risk in many ways, but I have chosen to classify the potential attacks in three groups:

1. *Easy for many*: The kinds of attack that many people can carry out, because no special skills or equipment are required.

    - Forging signatures. In privacy, with a sample to work against, it's just a matter of tracing. Ask your pre-school child to do it for you if you've lost the knack.
    - Getting a false ID. Freely available for R200-R300, with a photograph of your choice.
    - Opening a fraudulent account. You can even do it by phone.

Stealing a cheque in transit. At your premises, in the post, at the recipient's premises. By stealth or by brazenness (masquerading as a messenger with a stolen letterhead is a good one). Sometimes all you have to do is ask nicely at reception if there's a cheque for you.

2. *Easy if you make it so*: Some forms of attack are not always easy, but can be made so if you co-operate with the thieves.

- Stealing blank cheques
- Removing the information such as Payee name that you've put on the cheque
- Adding information, like "T/A A.N.Other Co. (Pty) Ltd" after whatever you put on the cheque.
- Stealing and using processed cheques to commit fraud
- Forging other value documents such as purchase orders, invoices and picking slips..

3. *Easy if you have special skills or access to special equipment*: Some things are easy to do if you have special skills or equipment, but to the bulk of criminals they are not simple. It is important here to keep re-assessing the situation because technology is moving so fast that today's special, expensive piece of equipment is tomorrow's standard small office kit. You must also accept that nothing I or anyone else can do will buy you 100% security. The goal has to be to make your documents more secure than the general run, so that fewer criminals will be tempted to target you.

    - High-quality scanning and printing (typesetter standard). This is unfortunately becoming cheaper and more accessible daily, but is not yet standard office equipment.
    - High-quality colour photo-copying. The best of them will reproduce detail at close to the resolutions of typesetters (1000 dpi or better).

This is the background then against which you need to assess your risks and understand your objectives. I offer two principles you should keep in view:

1. You will never eliminate all risk: your goal is to make an attack either costly enough or risky enough to outweigh the potential reward.
2. It's not very useful pouring resource into already strong areas if you are leaving holes elsewhere. Don't double-lock and bar the front door if you've left the windows open.

Objective: Prevention or Prosecution?

There are many security features, options and related bits of equipment tugging at your wallets, but seldom is the distinction drawn between prevention in the first place versus facilitating prosecution after the event. Whilst it is true that vigorous and certain prosecution and punishment would be effective deterrents, both are conspicuously absent in South Africa today. Being able to prove fraud on a "balance of probabilities" may at least give sufficient grounds for dismissal, but that is a relatively weak deterrent. I would argue from this that prevention should be your first line of defence, with the prosecution aspect being the second line.

When you are looking at methods to prevent fraudulently altered cheques being passed, you should also do an exercise: visit a bank in a busy centre at lunchtime on the last Friday of the month. Ask yourself if the measures you are

using or considering using will be effective in that situation, because that is when I would choose to pass a duff cheque.

Prevention

Protect your blank forms. A blank cheque is, you might say, as good as a blank cheque to a criminal. Cheque forms should be kept in a secure place with limited access, not left lying in a cardboard box under somebody's desk. Print under supervision, and/or put the printer in a locked room or lockable cabinet.

Permanently and irreversibly mark all cancelled or processed cheques. The best is to punch the word CANCELLED in machine-gun writing through the forms. Don't think that because a cheque has been processed and returned to you that it is no longer a threat. Recent changes to banking regulations have mitigated the risks here, since no cheque can be presented with any alterations. However, you must be sure that the cheque cannot be "laundered".

Paper security. Chemical sensitisation and fugitive inks are common features. Sensitisation causes the paper to discolour when various chemicals used to bleach out printed information are applied. Fugitive inks run and blotch as soon as certain kinds of liquids are applied and are used to print the background patterns on the cheques. There are two kinds of fugitive that react to water-based and chemical solvent-based liquids respectively, and you shouldn't assume your cheques have both.

Minimise handling. You should minimise handling of the forms from the time they are removed from the safe or strong-room to the point where they are completed, signed and delivered or posted. Every time cheques are moved from one place to another, or left on someone's desk awaiting signatures, presents another opportunity for someone to misappropriate one. The situation is worse if more than one person handles the cheques: not only are you increasing the likelihood of one of the people involved being dishonest, you are also making it harder to narrow the field of possible culprits when a problem is discovered. This is one reason why we more often get requests to sign cheques at the same time as they are printed. The most security-conscious customer we have keeps the cheques in a safe in the same secure room as the printer. At cheque-printing time, signatories come to the room to authorise the release of the cheques for printing and signing (through a combination of passwords and biometric verification). There are always at least two people in the room at any time when the cheques are out of the safe. The only movement of the cheques is when they are first brought into the room, and then when they are completed and sealed into envelopes they are removed from the room.

Printing and Fonts. Using strong, bold fonts that are not commonly used makes it harder for someone to scratch away what you put there and replace it with something else. The larger they are, the more work it is and the more of a mess they have to make, which is harder to cover up by using still larger fonts. Multicolour print is an excellent deterrent as it is far harder to tamper with or reproduce. Use a fresh ribbon: a tired old ribbon that prints characters in grey with fonts made up of dots with white space between them (typical of a 9-pin dot-matrix printer in fast draft mode) is an invitation to take your money.

Form of words. Fill in the amounts in full words: write "Four Thousand Two Hundred and Nineteen Rand", not "ZERO ZERO FOUR TWO ONE NINE". It makes it vastly harder to fiddle with the amount, which at least limits your exposure to the original face value of the cheque. Fill in blank space in both the Payee and the Amount fields. Leaving blank space after a Payee name invites the simple addition of "Trading As .....".

Don't use Laser printers. Laser printers deposit a plastic powder on the paper and then use heat and pressure (sometimes just pressure) to fuse the plastic and make it adhere to the paper. Note the term "adhere": i.e. it sticks to the surface. The degree of adhesion varies with fusing temperature and pressure, and the paper texture and humidity. It is not unusual to be able to lift off laser print with Prestik or magic tape, or some careful scratching. Another aid is to freeze the paper (dry ice and even liquid nitrogen have been used) which makes the toner plastic very brittle and able to be removed by spalling.

Carbon-ribbon typewriters. This is so secure, the typewriter even comes with a built-in lift-off ribbon! I would feel embarrassed making such an elementary observation, but I have seen cheques issued by a major insurance company completed in this way.

Daily bank reconciliation. Checking your account daily through electronic access through a modem is something most banks offer, and is one way to ensure that any cheque presented with a false number or altered value is picked up very quickly. At least one company, with very large cheque volumes, supply their bank with a tape listing the cheque numbers and amounts before the cheques are released. Their bank rejects any transaction that doesn't agree with the figures on the tape.

*Crossings and negotiability***.** The only way to make a cheque non-negotiable is to cross it Not Transferable **and** make it out to ABC Company (Pty) Ltd. Only. The trailing "only" is essential. Unfortunately, it also means that the slightest spelling mistake makes the cheque unable to be paid into the intended account: the details have to match the account name 100%. In practice, banks exercise discretion – but sometimes are too easy-going, so don't put too much faith in this.

Use continuous stationery. Where volumes permit it, have your cheque forms on continuous stationery. It is not possible to steal a cheque from the middle of a run of continuous stationery without it being obvious (it leaves a hole!), whereas with loose sheets you need constant checking to ensure no forms have gone missing.

Never assume anyone can be trusted. This is not an attack on the human race, but a reflection of the fact that you can never know what pressure someone is under. I know of a case where a long-term and trusted employee, with some 15 years service, was ordered to steal a cheque from her employees. She refused, and was beaten up very badly. She was then warned that if she did not steal a cheque, her children would be next. To most of us such threats might seem remote, but for many people they are very real.

Control Distribution. Post cheques if you must, but that is where a lot of cheques go astray. Often there is no choice, but then look carefully at everything we've covered so far! When people collect cheques, you should verify ID and get a signature.

Other documents. Put some thought into what other documents are valuable and could result in losses if fraudulently duplicated or altered.

Prosecution
This paper is intended to be about preventing fraud; not being in a position to prove it happened when you already know it has, so I will just list some of the commoner features that are used.

Watermarks
Holograms
UV Fluorescent paper and inks
Multicolour print
Smudge panels
Microprint

All of the above, when added to cheques, make it possible to tell unequivocally that a document is either a forgery or one that has been tampered with. (Note that multicolour print falls in this category as well as in the prevention category).

There will be times when it is very worthwhile to do this, and I do not decry them provided you keep in mind that they are not directly preventative methods.

EFT Payments
Our subject is cheque fraud, but no discussion of cheque fraud would be complete without some brief discussion of what some people see as the easy answer: eliminate cheques by using Electronic Funds Transfers.

EFTs are quicker, cheaper and cannot be stolen in transit. On the other hand there is resistance in some quarters to EFTs and not without reason.

- There is no physical audit trail. No paper to inspect for signs of wrongdoing.
- The skills needed to investigate possible EFT fraud are highly technical and not commonly available.
- The information transmitted to the bank contains human-friendly elements, but the most important one (the payee name) is ignored. Instead, the bank systems rely solely on the machine-friendly account number and branch code. A human checking the transaction file therefore gets a false sense of security if the details that the bank's computer ignores, are correct.

The convenience and low cost of EFTs (at least, as long as nothing goes wrong) means that they will continue to grow in usage. You can however consider applying some steps to reduce risk:

- Ensure strict authorisation controls.
- Try to have multi-factor authorization: e.g. password plus biometric (such as fingerprint), or password plus a smart card.
- Separate the duties of authorizing payments and capturing beneficiary details.
- Consider implementing forensic checking on the EFT payments: e.g. looking for payments to the same account number but with different payee details.

The DO's
DO have your cheques designed so that the important fields are clearly-marked boxes that are a snug fit around their content.
DO fill in the boxes completely with a fill character: a '*' or a custom fill chracter.
DO use a high-quality, high-impact printer with a fresh ribbon.

DO write out amounts in full words, not block words.
DO monitor your account daily to check amounts against cheque numbers.
DO use continuous stationery.
DO look after your used/cancelled documents with the same diligence you apply to your blank documents.

Summary

If anyone ever comes to your door offering you a perfect, fool-proof solution you can be sure you are talking to a liar.

This paper is intended to help you to assess the risks realistically and from there to determine your objectives and priorities. Once that has been done, you can apply the methods that give you your the trade-off between cost and protection that you are prepared to live with. No solution suits everyone, and no solution is perfect.