BUILDING TOMORROW™

Fraud Update 2014

RBS™

Useful Websites

"Keeping Your Business In Business" - information on fire and crime safety and disaster recovery measures

http://www.wmarsontaskforce.gov.uk/kybib-downloads.jsp

RBS Security Advice Centre

www.rbs.co.uk/corporate/banking/g6/online.ashx

Rapport - an extra layer of online security software

www.rbs.co.uk/corporate/ms/sc/online-security/rapport.ashx

Action Fraud

www.actionfraud.police.uk

Bank of England - banknotes information & training

www.bankofengland.co.uk/banknotes

HMRC - money laundering regulations

www.hmrc.gov.uk/mlr

UK Payments Industry - payment fraud advice

www.ukpayments.org.uk/payments_industry/payment_fraud

Website links correct at time of publication (October 2012)

RBS group is not responsible for the content of non-RBS group websites

RBS™

Corporate Markets

RBS
The Royal Bank of Scotland

Customer fraud awareness

Fighting cheque fraud

Cheque fraud has substantially increased over the years as fraudsters seek to exploit any opportunity to make money at our customers' expense. From the simple interception and alteration of cheque payee or amount details to cheque printing and forging of customer signatures, the technology used by the fraudster can be really effective. It can be astounding how a forged or altered cheque can look these days.

The Royal Bank of Scotland Group uses a whole range of anti-fraud prevention and detection processes in the ongoing fight against financial crime. But we also depend upon our customers to be vigilant and follow good practices in order to prevent such criminal activity.

Everyone's a potential target

Historically, a cheque was the business communities preferred choice as a means of payment for goods and services. This has to a large degree become more outdated as faster, cheaper and more efficient means of settlement are now available to customers for the payment of services or before releasing goods to a client.

The number of cheques being used has declined in preference to the use of electronic payment systems (e.g. CHAPS, BACS or desktop banking). Such systems having the added benefit of inherent additional security and anti-fraud measures absent in cheque payment methods.

Conversely, there has been a sharp rise in the number of attempted frauds against our customers' accounts where cheque payment continues. With fewer cheques being written and high value payments being settled electronically the fraudster now casts his net much wider than before.

The fact is cheque fraud has become more 'organised', advances in computer and printing technology, coupled with the relatively low cost of equipment, mean that the fraudster can now target almost any cheque written.

So what can be done and what part can you play to ensure that you do not become the target of a well orchestrated or even opportunistic fraud attempt?

It can make all the difference

Cheques are valuable and lack of care or attention in how they are stored and actually written, either by hand or computer printed, can lead to misuse by fraudsters and potentially to customer losses.

Remember to:

- always keep cheques in a secure place and always separate from the bank mandate and never leave cheques lying around unattended in public areas during the day
- compare underlying paperwork with all cheques written
- use cheques in serial number order
- ensure all cheques remain in the book and that none are removed from the middle or towards the back
- always account for spoiled cheques and destroy if appropriate
- undertake cheque stock audits regularly
- reconcile bank statements upon receipt and report anything unusual.

When writing cheques:

- begin writing/printing at the very left of the cheque
- when paying a cheque to a large organisation such as the Inland Revenue, do not make the cheque payable simply to that organisation. Add further details into the payee line e.g. Inland Revenue re: J Jones reference xxx. Draw a line through unused space on the cheque so unauthorised people cannot add extra details. The same principle would apply when making a cheque payable to a bank or a building society
- do not leave large spaces between words and rule out the space not used after the words in each line
- do not leave space between the '£' sign and the amount inserted in the figures box and again rule out any space not used after the numbers.

Non standard printed cheques

There are stringent anti-fraud and other industry standards that must be incorporated in all cheque designs for which the bank can provide full guidance.

And finally

Bank drafts are subject to the same issues as cheques and should be treated like any other 'cheque'. Remember it is advisable not to release goods before bank drafts are cleared for 'fate'.

It's a scam – You receive a cheque for far too much and are asked to send the balance back to the drawer by CHAPS. Be aware as the chances are you could end up with a bounced cheque and a debit to your account!

Note: This leaflet aims to assist to minimise the impact of fraud on your business. However relying on the information in this leaflet, although it may help reduce the risk of fraud, will not eliminate it, nor does it guarantee that fraud will not occur.

The Royal Bank of Scotland plc. Registered in Scotland No. 90312. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB. 087208 11/05

(1935-0805)

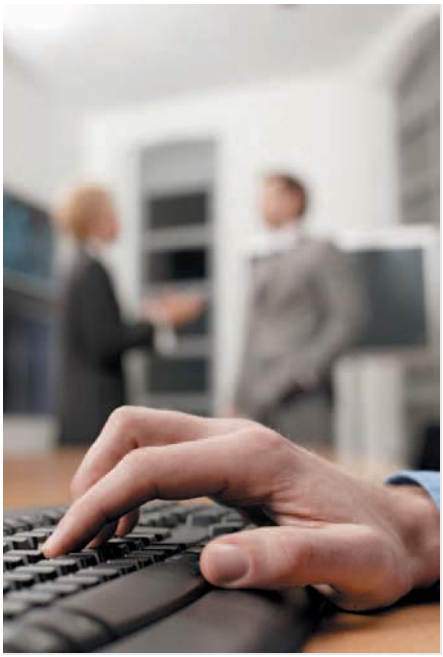
087208 12/08
779844

Corporate Markets

RBS
The Royal Bank of Scotland

Receiving payment by Cheque/Bank Draft

Fraud continues to evolve as criminals look for new ways to defraud their victims and everyone is a potential target. The Royal Bank of Scotland is committed to safeguarding your money and uses a wide range of fraud prevention and detection processes in the fight against financial crime. We also depend on our customers to **be vigilant and follow best practice** in order to help prevent criminal activity.



The risk facing you and your business

Traditional methods of payment, such as issuing cheques or drafts are used less in today's business world as faster, cheaper and more efficient means of paying for goods and services are now available.

The use of electronic payment systems has increased because these have the added benefit of security and fraud prevention controls that are not available when using cheques or bank drafts.

The reality is that advances in computer and printing technology, coupled with the relatively low cost of equipment needed to perpetrate fraud, make it relatively easy for a fraudster to target your business with a high quality counterfeit, forged or altered cheque or bank draft.

How can you make sure you receive payment for the goods or services you supply?

Drafts go through the normal clearing process like any other cheque. If you are offered a bank draft in payment, don't release the goods until you are sure the draft is genuine and has been paid. If accepting payment by cheque, unless it is properly drawn in accordance with the cheque guarantee card scheme, don't release the goods before you have positively established that the cheque will not be returned unpaid.

A forged, altered or counterfeit cheque or bank draft will ultimately not be paid.

Be wary:

- of a new customer and/or an unusually large order
- when a customer appears disinterested in the price/detailed description of goods
- where the goods are high value and/or easily re-sold
- if the buyer offers a cheque or bank draft already made out in your company's name for the full asking price, and wants to take the goods away immediately
- if you are put under pressure to release goods without undertaking essential checks
- of demands for next day delivery with no consideration for any additional costs and/or if the customer's address is local to you
- of phone calls on the day of delivery asking what time the goods will be delivered
- a customer who will only provide a mobile telephone number
- if the buyer offers a cheque or bank draft for a value above the asking price and asks you to return the overpayment in cash, via CHAPS or by some other means. It will be a scam.

Although it may be inconvenient, it may be better to lose a sale than the goods themselves.

The following are some alternative ways of transferring money that offer your business better security and are more convenient than cheques or bank drafts:

- CHAPS.
- BACS.
- Electronic Banking.

This leaflet aims to assist to minimise the impact of fraud on your business. However, relying on the information in this leaflet, although it may help to reduce the risk of fraud, will not eliminate it, nor does it guarantee that fraud will not occur.

The Royal Bank of Scotland plc. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB.
Registered in Scotland No. 90312. Authorised and regulated by the Financial Service Authority.

RBS087353 08/07

Customer Fraud Awareness

Alteration of creditor bank account details

Fraud techniques continue to evolve as criminals look for new ways to defraud their victims. Everyone is a potential target. The Royal Bank of Scotland is committed to helping you safeguard your money and uses a wide range of fraud prevention and detection processes in the fight against financial crime. We also help our customers remain **vigilant and to follow best practice** in order to help them safeguard their business.

Warning – alteration of creditors' bank account details

We have become aware that a number of customers have received fraudulent approaches purporting to be from existing suppliers or creditors. The fraudster advises that the bank details for the settlement of future invoices should be changed. These approaches have been made over the telephone, by letter, fax and by email. The request is not necessarily accompanied by any specific request for payment but if the request is acted on, then the next legitimate payment will be made direct to the fraudsters account. The fraud is sophisticated in that:

- Email addresses on letters use extensions similar to that of the genuine company but are in fact operated by criminals
- Fraudsters telephone the company they are targeting to ask for contact names so the correct ones appear on the letter
- Letters use the same logo, letterhead and style as the genuine company.

What do I need to do?

It is important that all requests for payment or to amend the bank details for the settlement of regular supplier payments or known creditors are independently validated before acting on the instruction.

- Closely scrutinise all requests for payment
- Contact the supplier or creditor to **independently** validate requests for payment or to amend bank details using contact details that are known or that have been obtained independently from the request you are seeking to validate e.g. Directory Enquiries or existing records within your business
- Do not amend any payment details until you are entirely satisfied with the authenticity of the request
- Alert those staff with access to financial systems to the above threat.

For further information about how to protect your business, please visit: **www.rbs.co.uk/onlinesecurity**

90062040

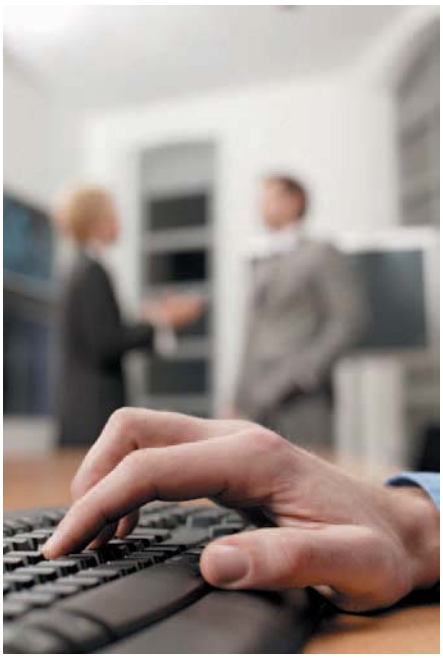
Corporate Markets

RBS
The Royal Bank of Scotland

Customer fraud awareness

Employee Fraud

The Royal Bank of Scotland is committed to safeguarding your money and uses a wide range of fraud prevention and detection processes in the fight against financial crime. We also depend on our customers to **be vigilant and follow best practice** in order to help prevent criminal activity.



Protecting your Business

Fraud is often considered to be an external threat, such as an attempt to obtain goods or services using a forged, altered or counterfeit cheque. However, whilst the majority of employees are honest and trustworthy, inadequate internal systems and controls expose a business to the risk of fraud being committed from within the organisation; possibly even by a long standing and trusted member of staff.

Trust is a hallmark of business life. There will always be a need for a company to place a certain degree of responsibility upon its employees. This means that a business must ensure that there are effective controls in place to safeguard company assets, including customer data and intellectual property, and deter staff from attempting to abuse their position for personal gain or on behalf of others.

Recruitment Checks

A dishonest employee could operate independently or organised criminal groups may attempt to place individuals inside an organisation. A robust and effective recruitment policy including comprehensive pre-employment screening is fundamental in helping to protect a business from employee fraud.

The following are some best practice pre-employment checks that a business can follow:

- obtain documentary evidence to confirm a prospective employee's name, address and right to work in the UK
- obtain a detailed employment history and where possible validate previous employment details, questioning any apparent gaps in the history
- request references
- validate listed qualifications
- undertake enquiries with credit reference and fraud prevention agencies.

Whilst a company may already undertake thorough checks for employees recruited directly, temporary staff or those recruited via agencies are not always subject to such stringent controls. Ensure any agency that your business uses performs pre-employment screening to the standard required by your business. Many organisations also run periodic post-employment checks.

Business Controls

In addition to pre and post-employment screening, consider implementing effective internal controls.

- control access to buildings and systems, where appropriate using unique identification and passwords
- restrict and closely monitor access to sensitive information, such as banking details, tender documents, pricing, and customer or supplier details
- have clear segregation of duties, particularly for staff authorised to set up, amend or make payments for the business
- use tiered authority and signature levels for payments
- regularly reconcile bank statements and other accounts
- periodically audit processes and procedures
- promote a culture of fraud awareness among staff
- adopt a 'zero tolerance' policy towards employee fraud.

Be alert to:

- a new member of staff who resigns shortly after joining
- any reluctance by an employee to take holiday entitlement
- any indication that a member of staff may be experiencing financial difficulties
- customer complaints regarding missing documentation or unrecognised transactions
- unusual changes in an employee's behaviour, personality or business performance
- a sudden change in an employee's lifestyle, unexplained wealth or a standard of living beyond their apparent means
- members of staff who consistently under-perform or exceed targets
- an employee's unusually close relationship with suppliers or contractors
- suppliers or contractors who insist on dealing with the same individual.

This leaflet aims to assist to minimise the impact of fraud on your business. However, relying on the information in this leaflet, although it may help to reduce the risk of fraud, will not eliminate it, nor does it guarantee that fraud will not occur.

The Royal Bank of Scotland plc. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB.
Registered in Scotland No. 90312. Authorised and regulated by the Financial Service Authority.

RBS087349 08/07

Corporate Markets

RBS
The Royal Bank of Scotland

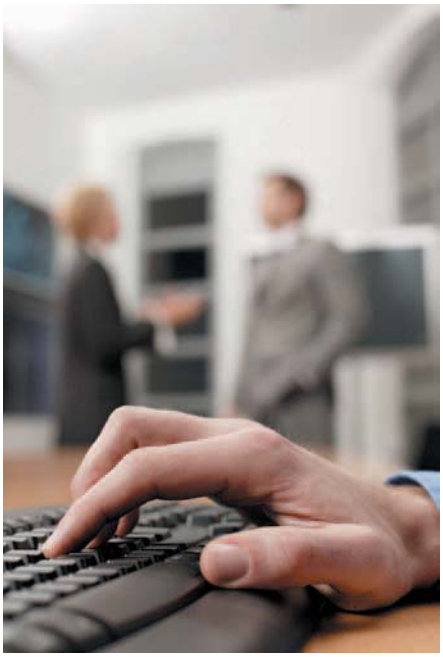
Customer fraud awareness

Computer and Internet Security

Fraud continues to evolve particularly as criminals look for new ways to defraud their victims and therefore *everyone is a potential target*. The Royal Bank of Scotland is committed to protecting your money and employs a wide range of fraud prevention and detection processes in the fight against financial crime. We also depend on our customers to **be vigilant and keep information secure** in order to help prevent criminal activity.

The risk

Historically, almost all financial transactions involved some form of face to face contact, but traditional methods of payments have declined in preference to the use of electronic payment systems. This does, however, potentially offer new opportunities to the fraudster.



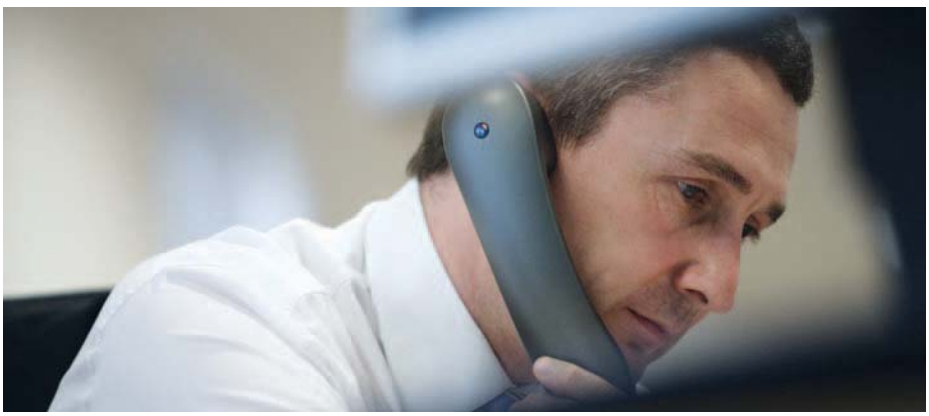
What are the main threats?

- **Phishing** – the practice of sending emails apparently at random, purporting to come from a genuine company operating on the Internet, *possibly a company that you or your business may deal with*, in an attempt to trick you into disclosing sensitive information. Such emails usually claim that it is necessary to 'update' or 'verify customer account information' via a link to a bogus web site. The criminals will then capture any information entered for their own fraudulent purposes. Bank customers have been the prime targets for this type of attack, but increasingly customers of other businesses who use the Internet have also become a target.
- **Trojan** – a type of computer virus which can be remotely installed on your computer without you realising. Fraudsters will typically try and trick you into following a link from an email to a malicious web site, where vulnerabilities in your web browser could be exploited to install the virus or other malicious software. Such emails will often contain a seemingly harmless subject such as a joke, greetings card or a current 'hot' topic.
- **Spyware** – software that could be installed on your computer via a Trojan or as part of another application, to monitor activity on the infected machine and report back to the fraudster. This could take the form of a **keystroke logger**, which is designed to read the keystrokes entered on your computer keyboard and capture passwords and other security information. You should be aware that although Spyware is often installed remotely, physical devices could also be directly installed on your computer.
- **Pharming** – Sophisticated malicious code could corrupt your computer and redirect any request for a genuine Internet site to a bogus site. The fraudster will then capture any personal details, including passwords, which you may exchange with the bogus site.

Despite these threats, the Internet remains a relatively safe channel though which to do business, provided users take adequate steps to protect themselves.

Staying safe online

- always keep passwords, PINs, and any other sensitive or financial details secure. This information should not be written down or shared and passwords should be changed regularly
- choose passwords that are easy for you to remember but impossible for others to guess. Avoid using anything that has an obvious connection to you. The most secure passwords are those that contain a mixture of letters, numbers and other characters, such as punctuation marks
- when contacting you, your bank or other financial institutions should not ask you to verify complete PINs or passwords
- never enter sensitive personal or business information such as account details, PINs or passwords via a web site link attached to an email
- know who you are dealing with:
  - be suspicious of all unsolicited or unexpected emails, *even if they appear to originate from a trusted source*
  - be alert to emails sent from an Internet type account (e.g. Hotmail, Yahoo, etc)
  - when keying sensitive data on a web site, ensure that it is secure – denoted by the prefix "https" and locked padlock or unbroken key symbol. You can check the authenticity of a secure web site by double clicking on the symbol
  - if in any doubt, contact the owner of the web site on a known or independently verified contact number
  - be careful about opening attachments or following links even if they appear to relate to innocent subjects, as these may contain a Trojan or another form of virus that could infect your computer.
- keep hold of your cash!
  - don't be conned by convincing emails offering you the "opportunity" to make some easy money. If it looks too good to be true, it probably is. Be especially wary of unsolicited emails from outside the UK – it will be much harder to verify the content or the source
- keep your computer secure:
  - install a personal firewall
  - employ up to date anti-virus software and run regular scans of your computer.
  - use a web browser (the program that lets users read and navigate pages on the Internet) that has been obtained from a reputable web site. Some web browsers offer added security to help protect you from Phishing attacks or Spyware
  - remember that you have no control over the security of a computer in an Internet café, airport lounge or any other PC to which the public have access or is owned by a third party
  - additional information on this subject is available from the following web sites:
    www.microsoft.com/security/protect
    www.banksafeonline.org.uk
    www.getsafeonline.org.uk
    www.bba.org.uk



This leaflet aims to assist to minimise the impact of fraud on your business. However, relaying on the information in this leaflet, although it may help to reduce the risk of fraud, will not eliminate it, nor does it guarantee that fraud will not occur.

RBS087347 08/07

Corporate Markets

RBS
The Royal Bank of Scotland

Customer fraud awareness

Identity fraud

Financial crime is growing fast and everyone's a target. That's why it's important that we continue to work together to beat the fraudster.

The Royal Bank of Scotland Group is committed to safeguarding your money and this factsheet explains how this can be achieved and gives a broader picture of where the threat of fraud may arise.

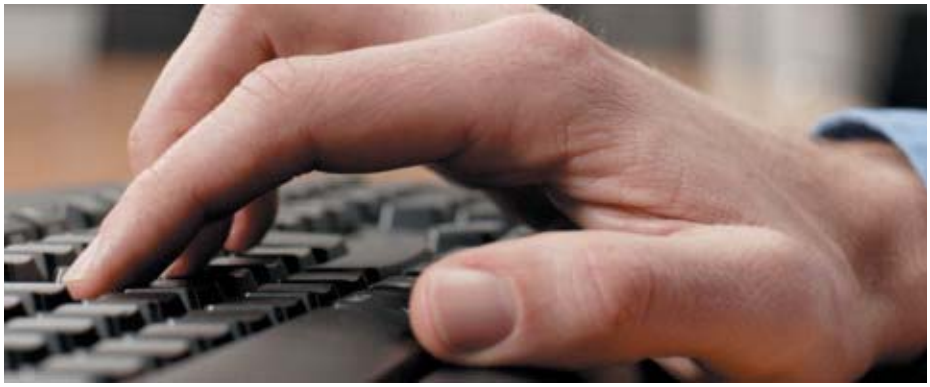
Friend or foe?

Recent years have seen a significant rise in the number of cases where fraudsters have successfully taken on the identity of bona fide customers and occasionally even their business. This is called 'Identity Fraud'. It is important for the business community to be aware of the nature of this threat and take steps to minimise its impact

Mobile phones and e-mail provide your business with two indispensable communication tools. These can create a 'feeling' of immediacy for response and exploiting this situation can provide a fraudster with anonymity and a quick route to success.

In a busy day-to-day office environment when your staff have many calls on their valuable time it can be easy to inadvertently forget to exercise the appropriate level of care and attention when dealing with enquiries for information from other parties. The positive human trait of 'being helpful' can become an Achilles' heel favouring the fraudster.

Please see the reverse to see how you can minimise the impact of fraud on your business.



Do:

- always verify with whom you are dealing before continuing any discussions or other form of communication
- fully consider the implications of divulging information to someone that you do not know – however compelling the reason or purpose behind the request
- understand what information you are being asked to provide – do you ever challenge such requests if the request seems unreasonable or unusual?
- verify if the approach is genuine by undertaking an independent call back to the originator using a known telephone number from your own records
- be wary of callers purporting to be phoning from the Bank – it could be a fraudster looking to get information about your accounts. If in doubt telephone your Corporate Service team if it's a transaction or processing enquiry or your relationship manager if the question relates to other banking matters
- question whether the e-mail that arrives in your 'inbox' really means that you need to turn around a reply immediately without further thought?
- shred documents containing personal or financial information before discarding – many fraud and identity theft incidences happen as a result of mail and rubbish theft
- protect your PC passwords – these should be memorised and not written down or shared with anyone, changed regularly and consider using a combination of letters and numbers
- try to avoid opening e-mails telling you that you have 'won a prize' or asking you to 'verify a statement'. If you do open an e-mail be wary of opening any attachments or links to web sites as these may contain viruses or other harmful programs
- be suspicious of non-business e-mails. An e-mail requesting your bank account information and password should be treated with suspicion. The Bank will never ask you for your Security number or Password in an e-mail. Never disclose this information to anyone.

Don't:

- supply information to anyone unless you are certain it is the usual business contact you would deal with – if it is not then challenge the request
- provide any information if it is not normal or the usual information you would be expected to provide in your business
- respond immediately to requests for information received via e-mail if the sender is not known to you
- use the telephone number a caller gives you to call them back – always obtain telephone numbers independently from your own business records
- give any banking or computer passwords or confidential information over the telephone unless you have initiated the telephone call and know whom you are dealing with.

Remember

If you are uncertain as to whether a particular approach for information is genuine, consider taking further action to validate the request, perhaps referring the matter to a colleague. Trust your instincts if it doesn't feel right it probably isn't.

Note: This leaflet aims to assist to minimise the impact of fraud on your business. However relying on the information in this leaflet, although it may help reduce the risk of fraud, it will not eliminate it, nor does it guarantee that fraud will not occur.

The Royal Bank of Scotland plc. Registered in Scotland No. 90312. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB.
(1934-0805)

087207 12/08
779818

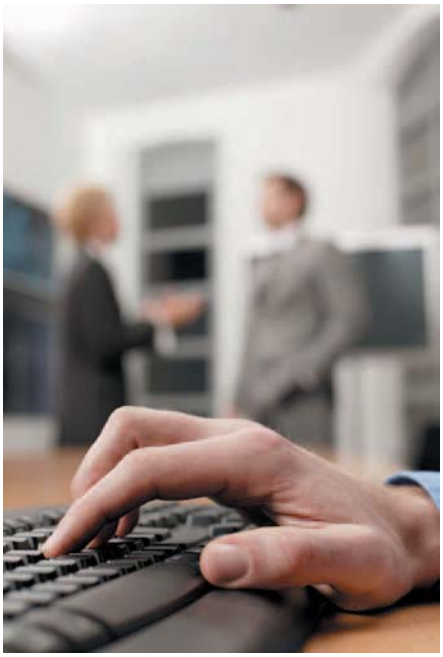
Corporate Markets

RBS
The Royal Bank of Scotland

Customer fraud awareness

Corporate Identity Fraud

Fraudsters are constantly looking for new ways to exploit any weaknesses in legitimate and successful businesses and *everyone connected with such businesses is a potential target*. The Royal Bank of Scotland is committed to safeguarding your money and employs a wide range of fraud prevention and detection processes in the fight against financial crime. We also depend on our customers to **be vigilant, follow best practice and keep information secure** in order to help prevent criminal activity.



How safe is your corporate identity?

Corporate identity fraud costs businesses millions of pounds per year. Criminals can file false documents with Companies House to change details of your company's directors and registered office and then use its identity for fraudulent purposes. The impact on your company could include correcting public records, repairing credit ratings and rebuilding supplier/client confidence.

The main risks

- all companies are at risk – however *those with less developed controls surrounding information security are more vulnerable*
- anyone can send a form to change company details, e.g. details of directors and the registered office
- Companies House accepts all filings in good faith. It is unable to undertake any checks to verify their authenticity
- once false information has been filed with Companies House, fraudsters can use a company's corporate identity to obtain goods and services on credit that are never paid for, or even trade on the good name and reputation of the genuine company.

What can you do?

To combat this type of fraud, Companies House has introduced a service called 'PROOF' (PROtected Online Filing) that enables a company to file specific forms electronically. Once a company is enrolled, any paper form submitted in its name will be rejected unless the company provides verification. Companies House also offers a monitoring service which allows a company to check which documents have been filed. For further information please refer to **www.companieshouse.co.uk**.

To help protect the identity of your company:

- regularly check the registered details of your company and its directors
- consider registering with Companies House for 'PROOF' and subscribing to 'MONITOR', the service that will issue an alert if any company information is changed
- your business should not rely solely on Companies House records when determining whether to provide goods or services to other businesses. Companies House maintains public records and is not a crime prevention or credit reference agency
- cross reference and validate Companies House information with other independent sources of information such as:
  - trade Associations
  - professional Bodies
  - the Internet. You should exercise caution, however, when using this channel to verify information, as fraudsters have been known to create false web sites. For added security, always attempt to corroborate information via a number of different sources.

This leaflet aims to assist to minimise the impact of fraud on your business. However, relying on the information in this leaflet, although it may help to reduce the risk of fraud, will not eliminate it, nor will it guarantee that fraud will not occur.

The Royal Bank of Scotland plc. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB.
Registered in Scotland No. 90312. Authorised and regulated by the Financial Service Authority.

RBS087348 08/07

Corporate Markets

RBS
The Royal Bank of Scotland

Customer fraud awareness

Plastic Card Fraud – Card Present Transactions

Our business customers are the front line against card fraud, which can result in a double theft: against the genuine cardholder and against the company that the fraudsters may trick into supplying goods and services.

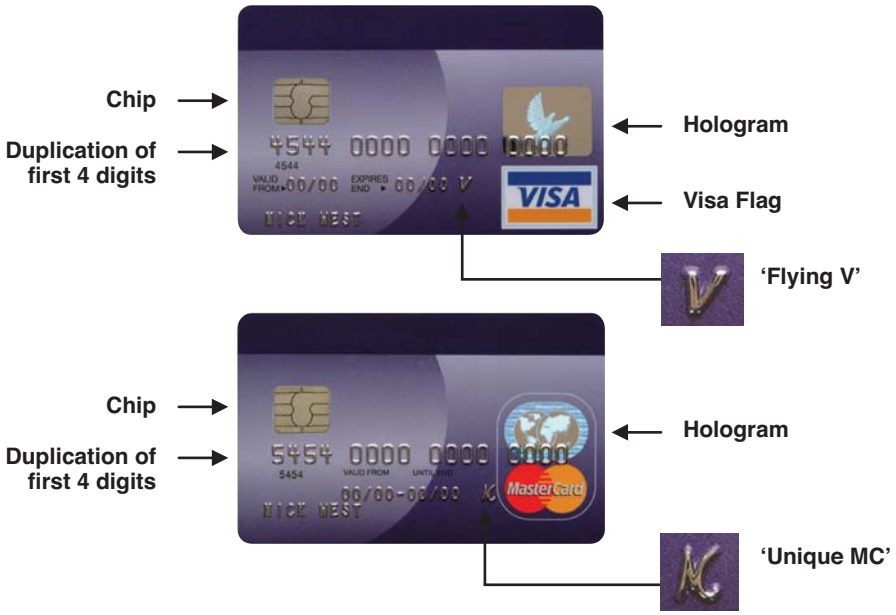
Together, The Royal Bank of Scotland and the payment card industry are doing all we can to fight fraud and safeguard your money. We also depend on our customers to **be vigilant and follow best practice** in order to help prevent criminal activity. This guide is designed to offer some quick and simple checks to help you verify the authenticity of the card and cardholder and receive payment for the goods and services that you supply.

Remember: authorisation does not guarantee payment. It will only establish that, at the time of the transaction, there are sufficient funds available to cover the payment and that the card has not been reported lost, stolen or compromised in any other way.

For **Chip & PIN transactions**:

- follow the prompts on your terminal
- ask the cardholder to enter their PIN
- if a Chip & PIN card is not processed correctly, you may be held liable for the transaction in the event it is later confirmed to be fraudulent.

Not all cards in circulation have chip technology. If the card is **not Chip & PIN enabled**, you should take the opportunity to check the security features as you have sight of the card.



Please note that Visa Electron cards do not carry the 'Flying V' symbol.

An ultra violet lamp can be used to check for the appropriate mark:

Please note that some Visa Electron cards do not have ultra violet features

Although current Visa and MasterCard designs will remain in circulation for some time, newly issued cards are being re-branded with updated designs and security features.

- Visa has introduced a new logo which will appear in place of the Visa flag on the front of the card:

VISA VISA

- on a Visa card that has the new logo, the ultra violet image will be seen within the logo
- the word 'Visa' repeated on the signature strip will also show up under an ultra violet lamp
- the hologram or holographic magnetic stripe may appear on the reverse of a Visa or MasterCard card
- both the unique 'Flying v' and the 'MC' embossed characters may not be present on the front of the card
- more logo placement options and vertical orientation of the card and the logo are also available.

Be aware that some fraudsters spend a long time building credibility and are very confident and plausible.

Security checks

- be alert to customers seeming to make indiscriminate purchases – especially if the goods can be easily re-sold
- check that the title on the card matches the person presenting it
- check that the last 4 digits of the card number and the signature on the card match those on the terminal receipt
- look for any tampering of the signature strip
- be aware of cards that have been signed in felt tip pen, as this may be an attempt to cover the genuine signature. All cards should be signed in ballpoint pen.

Be particularly wary of:

- a customer who offers two cards as payment for one order *– this is not permitted under card scheme rules*
- a customer who provides several cards for payment after the initial and any subsequent authorisation requests have been declined.

Remember: make a 'Code 10' authorisation call if you are suspicious about the card or presenter.

For further guidance please refer to your Merchant Operating Instructions. Additional information is also available at:
www.streamline.com
www.cardwatch.org.uk.
www.visa.co.uk
www.mastercard.com/uk

This leaflet aims to assist to minimise the impact of fraud on your business. However, relying on the information in this leaflet, although it may help to reduce the risk of fraud, will not eliminate it, nor does it guarantee that fraud will not occur.

The Royal Bank of Scotland plc. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB.
Registered in Scotland No. 90312. Authorised and regulated by the Financial Service Authority.

RBS643063 11/07

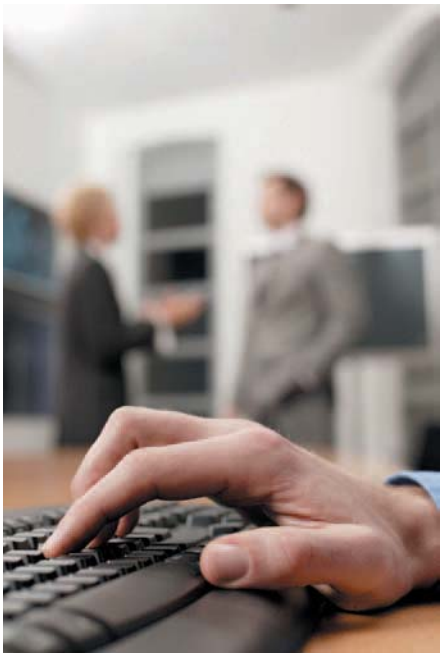
Corporate Markets

RBS
The Royal Bank of Scotland

Customer fraud awareness

Plastic Card Fraud – Cardholder Not Present (CNP)

Our business customers are the front line against card fraud, which can result in a double theft: against the genuine cardholder and against the company that the fraudsters may trick into supplying goods and services.



Together The Royal Bank of Scotland and the payment card industry are doing all we can to fight fraud and safeguard your money. We also depend on our customers to **be vigilant and follow best practice** in order to help prevent criminal activity. This guide is designed to help you verify the authenticity of a transaction and receive payment for the goods and services that you supply.

CNP transactions by their nature present a higher risk to your business, because there is no opportunity to physically check the card or meet the cardholder. Although the majority of payments will be completely genuine, this type of transaction is becoming more appealing to fraudsters because it increases the opportunity for anonymity.

Remember: authorisation does not guarantee payment. It will only establish that, at the time of the transaction, there are sufficient funds available to cover the payment and that the card has not been reported lost, stolen or compromised in any other way.

Best practice guidelines:

- ensure that your terminal has both the Address Verification Service and Card Security Code checking function enabled. These check the cardholder's address and the unique three-digit number found on the reverse of the card, usually within the signature strip
- call back cardholders using an independently obtained or verified land line number. Telephone numbers can be checked by dialling directory enquiries and/or using on-line residential or business directory services
- goods should be delivered to the cardholder's registered and verified address and never released to a third party, e.g. taxi drivers or couriers. If the customer wishes to personally collect the goods you should process the transaction on a cardholder present basis.

Be particularly wary of:

- a new customer placing a large order and who appears disinterested in the price/detailed description of goods
- a customer being prompted by a third party in the background
- a customer who hesitates when asked technical questions about the goods they are purchasing
- demands for next day delivery with no consideration for any additional costs and/or if the customer's address is local to you
- phone calls on the day of delivery asking what time the goods will be delivered.
- a customer who will only provide a mobile telephone number
- a customer who offers two cards as payment for one order *– this is not permitted under card scheme rules*
- a customer who provides several card numbers after the initial and any subsequent authorisation request has been declined.

For further guidance please refer to your Merchant Operating Instructions. Additional information on this subject is also available at **www.Streamline.com** and **www.cardwatch.org.uk**.

This leaflet aims to assist to minimise the impact of fraud on your business. However, relying on the information in this leaflet, although it may help to reduce the risk of fraud, will not eliminate it, nor does it guarantee that fraud will not occur.

The Royal Bank of Scotland plc. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB.
Registered in Scotland No. 90312. Authorised and regulated by the Financial Service Authority.

RBS087351 08/07