Helping you to protect your company against fraud and financial crime

HSBC takes fraud and other financial crimes very seriously. Even though we have market-leading fraud detection systems, we want you to be aware of the different ways criminals may try to steal not just your money but also your company's identity.

Here are a few tips on how to avoid becoming a victim of fraud. Please read in conjunction with our Business Terms and Conditions.

Business Email Compromise (BEC) Fraud

The Business Email Compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform payments using an email from a company owner (CEO or CFO) as the authority to carry out the payment. Little does the payment processor know that the email is not a genuine company request.

There are two variations of this fraud type, which are as follows:

- **Email spoofing** – This involves the manipulation of an email address to make the senders email address appear to have originated from someone or somewhere other than the actual source.
  - The fraudsters spoofs the vendors email to submit the modified invoice. It doesn't require compromising the vendor's email system, but instead sends the invoice from an email that is so close to the domain of the vendor that most people would miss the change, for example,
  - @CompanyABC.com instead of @CompanyACB.com.
- **Compromised Email Account** – This involves the compromise of an executives email account within the organisation, such as the CFO (Chief Financial Officer). The fraudster sends a request for a payment from the compromised email account to another, often junior employee to action.

Remember,

1. Make sure staff are aware to check the email address the payment request is sent from, and have suitable checks in place to verify any new payment request received by way of email.

2. Always regularly review your organisations controls to make sure that you have suitable payment controls in place to not fall victim to this type of fraud.

Payment Diversion / Invoice Fraud

This type of fraud occurs when a fraudster tricks an organisation into changing the bank account payee details for a payment. Fraudsters pretend to be a regular supplier of the organisation and inform them of a change of bank account details.

This can include:

- creating bogus customer records and bank accounts so that false payments can be generated.

How to reduce your organisation's risk of becoming a victim of invoice fraud:

- Make sure staff that process invoices and requests are aware of this scenario when undertaking amendments to long standing payment instructions.
- Always verify changes to financial arrangements with a supplier directly using established contact details you have on file.

HSBC

"Phishing"

This is where people receive emails directing them to websites where they are asked to provide confidential personal or financial information. Whilst these emails may appear to come from a legitimate site, these emails are designed to steal your personal information and use it to access your accounts. This is known as Phishing. Do not reply or click on a link in an email that warns you that your account may be shut down unless you confirm your personal information. Instead contact the company, in a way that you are sure is genuine such as an authenticated telephone number.

You should delete these emails immediately

"Vishing"

This involves a fraudster making phone calls to a company, posing as bank staff, the Police, regular supplier / client or other officials in a position of trust. The call may be made to coerce a company financial controller into:

- Sending their money to another account often purportedly for 'safe keeping' or 'holding'.
- Withdrawing cash and handing it over to the fraudster for investigation.
- Giving personal financial information, which can then be used to gain access to your company bank accounts.

Remember,

1. Be wary of unsolicited approaches by phone, especially if asked to provide any of your company's restricted information.

2. If you are suspicious, don't be afraid to terminate the call and, say no to requests for information.

3. It takes two people to terminate a call, so ensure the caller has also hung up and you have a clear line, you can use a different phone line to test the number.

4. Fraudsters can use 'call spoofing' to deliberately falsify the telephone number relayed on the caller ID to show as a genuine bank number.

5. HSBC will never call you to ask you to generate a Secure Key code by pressing the yellow button or ask for your PIN number.

6. Never share company security details beyond authorised staff. It is important to keep your account and security details safe.

Criminals may already have basic information about your company in their possession (ie name, address, account details), do not assume a caller is genuine because they have these details or because they claim to represent a legitimate organisation.

Cheque Fraud

This fraud type involves the alteration, forgery or counterfeiting of cheques drawn out your Business account. If your company or your business partners are using cheques, to help your company not become a victim of cheque fraud, below are some tips on how to try and minimise this risk:

- Check your cheques. Add extra information to them, like an account reference number.
- Use your full signature when you sign your cheques – not just initials.
- Match your cheque counterfoils to your statements. Let us know about discrepancies as soon as possible.
- Keep any spare chequebooks in a safe place.

Protecting your Card

- Sign and activate your new card as soon as you receive it.
- You can activate your card either through internet banking, by contacting your Relationship Manager (RM) or by using an HSBC ATM (for Visa debit cards, unless a new PIN has been issued).
- Contact your Relationship Manager (RM) if your replacement card does not arrive a week before your old one expires.

Protecting your PIN

- Never write down or otherwise record your PINs and other security details in a way that can be understood by someone else.
- Destroy your PIN advice as soon as possible.
- Choose a PIN number that cannot be associated with you and isn't a sequence such as 1234 or 1111. Ideally choose a random combination or a sequence of numbers which are important to you.

Protecting yourself at the ATM

- A device may have been fitted to the ATM, which could enable the fraudster to steal your card or capture the information contained within the magnetic strip. If you notice anything unusual attached to the ATM, do not try to remove it. Move away from the machine and call our Lost and Stolen Cards team (using the number in the useful contacts below or the police.
- Always stand close to the machine and use your hand as a shield over the keyboard. Criminals may try to watch you entering your PIN, before trying to steal your card.
- If the cash machine does not return your card, do not re-enter the PIN. Report the loss of your card to your Relationship Manager (RM) immediately.

Protecting your company cards over the Telephone

- When making card payments over the phone, you should have your card in front of you as you may be asked information such as expiry date, issue number and the three-digit security code on the signature strip. However, NEVER divulge your PIN over the telephone, even if asked.
- Try to avoid saying your card information in public places where people may overhear.
- Request postal or email confirmation of the transaction.

Protecting yourself whilst using your card in person

- Try to use your hand as a shield when entering your PIN.
- If you encounter any problems whilst using your card, please contact your Relationship Manger (RM).
- Please keep your cards in a secure place at all times.

Protecting yourself Online

- Only shop at secure websites – ensure that the security icon (a locked padlock) is showing in the browser window if on a page requesting input of personal information.
- Print a copy of your order confirmation. A postal address and telephone number should also be available.
- When paying online with a credit card, always sign up with Mastercard Securecode or Verified by Visa. These provide personal password protected services.

Protecting your Passwords

- Use different passwords for different systems.
- Do not be tempted to use passwords that can easily be guessed such as children's names or birth dates.
- Never write down your passwords, however if you have no alternative, record them in a way that cannot be understood by anybody else.
- Instead of using your Mother's Maiden as your memorable name, consider using the name of your favourite cartoon character or another fictional person.
- Use a mixture of numbers and letters of upper & lower case to strengthen your password.

…and protecting yourself and your business against Identity Theft

Using a variety of methods, criminals may obtain important pieces of personal and identity data such as credit card numbers, expiry dates, dates of birth or mothers' maiden names. This information can be used to gain access to bank accounts or open new credit facilities.

Help to minimise this risk by following these simple steps:

- Shred all receipts or any letters, which contain your business name and address or personal information. Switch off your postal statements to prevent unnecessary documents being sent via the mail.
- Set up a telephone security number, as this is a secure way for us to identify you when you call us.
- Don't give your telephone security number out to anyone who contacts you. HBSC will NEVER ask for your telephone security number if WE call YOU.
- If you have lost or had stolen important documents such as a passport, consider registering for the CIFAS Protective Registration Service.

Should your company become a victim of fraud, please remember to report the incident to HSBC as soon as possible via your Relationship Manager (RM).