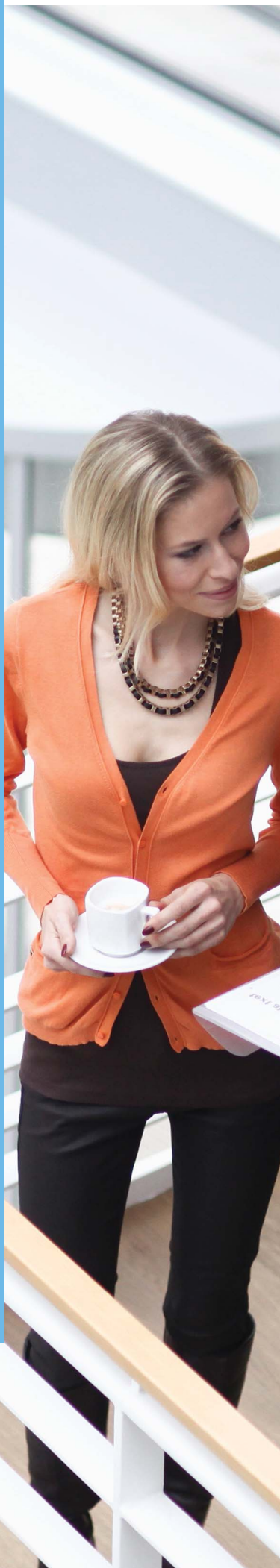
globalpayments

www.globalpaymentsinc.co.uk

HINTS AND TIPS FOR PROTECTING YOUR BUSINESS AGAINST **FRAUD**

Fraudsters have many ways of targeting businesses, whether anonymously online, posing as a customer or in your employment. This guide aims to provide you with some popular hints and tips for identifying potential fraud to help you protect your business.



TIP 01

BE SCEPTICAL

If it sounds too good to be true it probably is. Always approach deals/new business opportunities/transactions with an open, inquiring and questioning mind.

TIP 02

KNOW YOUR BUSINESS INSIDE OUT

By having a thorough understanding of your business it will ensure that you know:

- how it operates
- the staff you employ
- the products and services it provides
- your target market and your business obligations, both legal and regulatory

All this will help you detect when something is not right.

TIP 03

KNOW YOUR CUSTOMERS AND SUPPLIERS

Understanding who you do business with will help you identify occasions where a seemingly ordinary business request or transaction looks out of the ordinary for that customer or supplier and may be potentially fraudulent. It is important that you conduct due diligence using a risk based approach – verify the legitimacy of the customer/supplier details you have stored on file/record as well as online searches.

TIP 04

IDENTIFY AREAS WHERE YOUR BUSINESS IS VULNERABLE TO FRAUD

Take time to imagine how a fraudster may target your business, internally and externally and consider testing the systems you have put in place to reduce your exposure to fraud/risk. Train your staff on those systems and review them on a regular basis.

TIP 05

DEVELOP A STRATEGY AND TALK ABOUT FRAUD

Consider a prevention strategy that details controls and procedures to prevent and detect fraud that is adequate and appropriate for your business. Staff will look to you for guidance as to what behaviour is acceptable. Talk about fraud with your staff, suppliers and any other contacts. Your staff should understand the risks and impact of any losses on the business and to themselves.

TIP 06

TAKE EXTRA CARE WITH ALL THINGS CYBER

With increasing threats from cybercrime make sure that your business technology/website is adequately protected against attacks. Make sure that you back up your systems in case they go wrong.

TIP 07

UNDERSTAND YOUR FINANCES

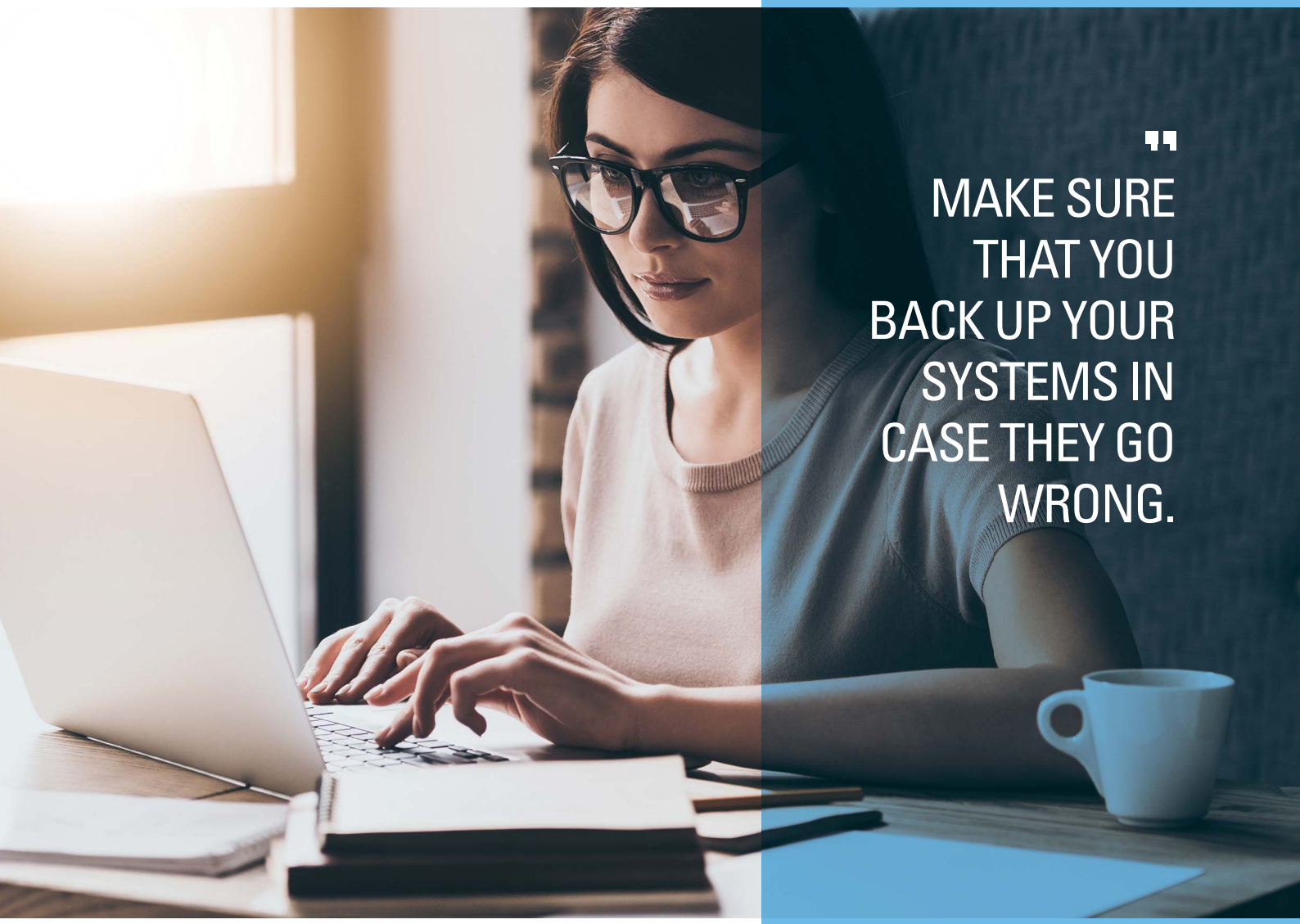
Understand how money leaves your business/ bank account e.g. methods of payment, who has the authority to make those payments and who checks that those payments are legitimate. Always check your bank statements!

> MAKE SURE THAT YOUR BUSINESS TECHNOLOGY / WEBSITE IS ADEQUATELY PROTECTED AGAINST ATTACKS.

TIP 08

SECURE AND PROTECT YOUR PROPERTY

This includes laptops/computers, smartphones and intellectual property. Consider obtaining business insurance to cover these items if they are compromised and/or stolen. Using and maintaining inventories can also protect your business.



"MAKE SURE THAT YOU BACK UP YOUR SYSTEMS IN CASE THEY GO WRONG.

"

HAVING AN ACTION PLAN IN PLACE WILL HELP LIMIT THE LOSSES TO FRAUD

TIP 09

DEVELOP AN ACTION PLAN

You should consider where you might need professional or legal advice. While prevention is better than the cure, it is important for you and your business to be prepared for the worst. Having an action plan in place will help limit your losses to fraud and help ensure that your business doesn't suffer damaging losses.

TIP 10

ALWAYS REPORT FRAUD AND GET HELP

Action Fraud is the UK's national fraud reporting centre where you should report fraud if you have been scammed or defrauded. They are a central point of contact for information about fraud and financially motivated internet crime. Report online at **actionfraud.police.uk** or by telephone on **0300 123 2040**. Report to your local police if the suspect is known or still in the vicinity.

TIP 11

CHECKING CARDS – WHEN THE CUSTOMER IS PRESENT

When customers are paying by card, whether debit or credit card, check the following:

- That the printed digits above or below the first four embossed card number are the same. This security measure features on both MasterCard and Visa cards. With counterfeit cards these four digits are often missing or rub off if you run your finger over the digits. On payment cards that have been counterfeited, they might not match the embossed details
- Always check the title on the card matches the gender of the person presenting it
- Check cards under ultra violet (UV) light which will show any anomalies. Most genuine cards have special inbuilt marks on them which only show up under UV light. If these security features are not visible and correct under UV light then the card is counterfeit
- Check card receipts to make sure that the number on the card matches with the number on the receipt. If you are accepting a non chip and pin card payment, keep hold of the card while the person is signing. This is so a fraudster cannot easily copy the signature

If you are at all suspicious of any of the above and you believe that your customer checks have failed, you should contact your card terminal provider/acquirer Authorisation Centre.

TIP 12

MANDATE FRAUD

This occurs where someone tricks you into altering details of a direct debit, standing order or bank transfer mandate by purporting to be an organisation you make regular payments to e.g. a business supplier. Verify and corroborate any request to change supplier's bank details with the organisation directly, using established contacts you have on file wherever possible.

TIP 13

KNOW YOUR STAFF

Employee fraud poses a serious risk to your business and if your business is small, employee fraud can have a greater impact on the success of the business. Be aware of possible employee theft indicators –

- New member of staff resigning shortly after joining
- Staff with financial difficulties
- Staff with a sudden change in lifestyle – cars/ holidays etc
- A pattern of customer complaints
- Change in behaviour by a staff member e.g. retracting from others
- Performance drops
- Suppliers/contractors insist on dealing with one individual
- Staff on sick leave but working elsewhere
- Abuses of flexible working time systems
- Computer misuse
- False references or false qualifications used to secure employment

TIP 14

FRAUDULENT REFUNDS

Members of staff/customers have been known to process refunds to their own card/s.

- Make sure that you control who has access to the supervisor/refund PIN
- Change the generic PIN that comes with a new card processing terminal
- Ensure that this is changed regularly particularly upon staff leaving
- Ensure that you have processes in place to help you spot unusual refund activity
- Check the End of Day/Z totals – ensure any refunds are for genuine customers/known transactions

VERIFY AND CORROBORATE ANY REQUEST TO CHANGE SUPPLIER'S BANK DETAILS WITH THE ORGANISATION DIRECTLY

TIP 15

PHONE SCAMS

If anyone calls your business purporting to be a card processing terminal engineer, from Visa or MasterCard or even your card processing terminal provider/acquirer, asking for card details of the most recent transactions processed do NOT give them any information at all and alert your card processing terminal provider/acquirer.

A variation on this is where the caller will state that there is a fault with your terminal and that they need to test it by asking you to process a card transaction using one card and then a refund using a different card. Do NOT process such transactions as your business will suffer a financial loss to the value of such transactions. Alert your card processing terminal provider/acquirer.

TIP 16

CUSTOMER DISTRACTION

A fraudster may attempt to distract you when they are entering their PIN into the card processing terminal. This is so they can enter a dummy/false authorisation code. Be wary of a customer that holds onto the card processing terminal for longer than is strictly necessary.

TIP 17

REFERRED TRANSACTIONS

Occasionally when completing a card transaction on your card processing terminal, you may receive a message: 'CALL AUTH CENTRE' on the terminal screen. This is because the card issuer wishes to undertake further verification of the customer/cardholder. Should this occur contact your Authorisation Centre at once and NEVER accept an authorisation number from the customer or from a caller claiming to be from the cardholder's bank. Such codes are not genuine and may result in a financial loss to your business.

Global Payments is HSBC's preferred supplier for card processing in the UK.

Global Payments is a trading name of GPUK LLP. GPUK LLP is authorised by the Financial Conduct Authority under the Payment Services Regulations 2017 (504290) for the provision of payment services and under the Consumer Credit Act (714439) for the undertaking of terminal rental agreements.
GPUK LLP is a limited liability partnership registered in England number OC337146. Registered Office: 51 De Montfort Street, Leicester, LE1 7BB. The members are Global Payments U.K. Limited and Global Payments U.K. 2 Limited. Service of any documents relating to the business will be effective if served at the Registered Office.

Issued by Global Payments, 51 De Montfort Street, Leicester, LE1 7BB. GP419