Fraud SMART

Protect Your **Business** from Fraud

www.FraudSMART.ie

Banking & Payment Federation Ireland

supported by

Led by Banking & Payments Federation Ireland, FraudSMART is a joint initiative developed by the banking sector. Sign up on www.FraudSMART.ie for alerts on current fraud trends that may impact your business.

Contents

FraudSMART

Most businesses would like to think that they are protected against fraud but unfortunately SMEs continue to be a target of financial fraud and scams. The majority of fraudsters use telephone, text messages and emails to commit the crime and new approaches are continually emerging that businesses need to be on the alert for.

Fraudsters take advantage of busy work schedules and create an unnecessary urgency to make you act without taking the time to do your checks. You are likely to get an email or a phone call from somebody you "know" and "trust". They may also use information that is publicly available to trick you into trusting them.

With many advances in technology to prevent banks and large companies being targeted, many fraudsters have turned their focus towards businesses and consumers directly.

FraudSMART aims to raise awareness of the latest financial fraud activity and provide simple advice on how best to protect your business

Log onto FraudSMART.ie for a wide range of information and advice to avoid being scammed and sign up for alerts on current fraud trends that may impact your business.

www.FraudSMART.ie
FraudSMART
@FraudSMART
@FraudSMART

Top Tips to prevent fraud in your business

Be Informed

- Ensure employees are fraud aware and understand controls and procedures in place to prevent fraud.
- Don't assume you can trust caller ID. Phone numbers can be spoofed so it looks like a particular company is calling even if it is not the real company.
- Fraudsters may already have basic information about you or your business (e.g. name, address, account details). Do not assume a caller is genuine because they have these details.

Be Alert

- Be wary of payment requests that are unexpected, irregular or require changes to bank account details.
- Exercise caution when forming new relationships with potential customers, undertake appropriate due diligence.
- Check your statements regularly and report unusual transactions to your bank immediately.

Be Secure

- Don't allow yourself to be rushed. Take your time to do the relevant checks.
- If a supplier/service provider requests bank account details to be changed have a verification process in place before making payments.
- Ensure security and software is regularly updated and maintained using official and reliable software.

Email Scams

Invoice Fraud

Fraudsters pretend to be a supplier or service provider in order to trick you into changing bank account payee details on your online banking. An employee receives an email informing them of the new bank account details. Often there is no request for payment but all future payments will go to this account controlled by the fraudster.

Your business orders from a supplier

Fraudster uses malware to access the details

Fraudster sends a fake invoice with new bank account details that look legitimate

Your business pays money to the "new bank account" i.e. the fraudster's account

Be Informed

- Have a verification process in place before changing saved bank account details of your suppliers or service providers.
- Verify the change by contacting a known contact in the company directly, use contact details held on record or a contact number on the company's website. Do not to use the contact details on the letter/email requesting the change as these could be fraudulent.
- Inform employees of this fraud so they are alert to it and can avoid it.

Be Alert

- Fraudsters can change an email address to make it look like it has come from someone you email regularly. Look out for different contact numbers and/or a slight change in the email address e.g. .com instead of .ie as these may differ from previous correspondence.
- The first contact may inform you of a change in bank account details but not request payment. This ensures that all future payments are sent to the new account.

Be Secure

- Fraudsters may have found information regarding contracts and suppliers on your company's own website. You should consider if this information really needs be on your website for fraudsters to utilise.

CEO/Executive Impersonation Fraud

The fraudster impersonates the CEO or a Senior Executive from your company. A legitimate email account is hacked to get an employee to unwittingly transfer funds.

For example, the fraudster will hack into the CEO's email account and send an email to an employee requesting them to make a payment to a supplier. Bank account details may be provided in the email or an existing supplier who has recently sent a change request to the finance team. This results in the funds ending up in the fraudster's account and not your supplier's.

Be Informed

- Always check with the person you believe sent the email that it is from them, no matter how senior or busy!
- Do not do this by email in case their account has been hacked. Instead, make a phone call, ask in person or use some other trusted communication method.

Be Alert

- Be wary of payment requests that are unexpected or irregular, whatever the amount involved.
- Verbally verify bank account change requests from suppliers. Don't fall foul of the fraudster's tactic to send the email when the "sender" is away from the office making it difficult to verify with them. Do not email them.

Be Secure

- Don't allow yourself to be rushed. Take your time and do the relevant checks.
- If in any doubt, do not make the payment, however urgent it may seem or whatever the suggested outcome(s).

How CEO Fraud Can

The Start

The fraudster spoofs your domain

Fraudsters often troll companies for months to gather the data necessary in pulling off a successful attack

The Phish

Spoofed emails are sent to high-risk employees in the organisation

To: Finance Dept.

Urgent transfer request. Please send €100,000 to new acct.

IE41 RANW 940109 20182012

To: CFO

Please pay this time-sensitive invoice. I'm on holidays and will be unavailable, no need to respond. - Your CEO

To: HR Dept.

I need a PDF copy of ALL employee P30s for Revenue ASAP!

The Response

Target receives email and acts without reflection or questioning the source

I better get this payment to the new account!

It's from the CEO, I'll take care of this for her!

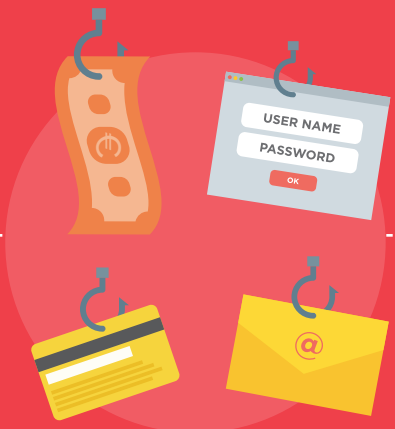
Sounds important. I'll send these right away!

Impact Your Business

The Damage

Social engineering was successful, giving hackers access to what they were after

This leads to fraudulent wire transfers



The Result

The fallout after a successful attack can be highly damaging for both the company and its employees

Resulting damage:

- Money is gone and often not recovered
- Data Protection breaches may result
- Legal action
- Intangibles - tarnished reputation, loss of trust, etc.

So... Think Before You Click

Phone Scams

Vishing (Voice and Phishing) is a phone scam where fraudsters target a business by phoning and claiming to be your bank, card issuer or service provider e.g. computer support looking to talk you through a procedure over the phone to "upgrade your system" or somebody claiming to represent your payment terminal maintenance.

Fraudsters try to extract details such as information about your computer system, business details, debit or credit card details, PIN number, online banking details and passwords. This can then be used to gain access to company bank accounts, carry out transactions or steal personal customer information.

Be Informed

- Never divulge personal or business information until you have validated that the caller is a genuine representative of the organisation they claim to represent. Hang-up, look up the number independently and call back, make sure you hear a dial tone before you dial.
- Don't assume you can trust caller ID. Fraudsters can spoof their numbers so it looks like they are calling from a particular company, even when they're not.
- Your bank or the Gardaí/Police will never ask you for your credit or debit card PIN number or full online banking password.
- Your bank will never request that you withdraw money to hand over to them or transfer money to another account, even if they say it is for safekeeping.

Be Alert

- Remember that it takes two people to terminate a landline phone call; you can use a different phone line to independently check the caller's identity.
- Fraudsters may already have basic information about you or your business in their possession (e.g. name, address, account details), do not assume a caller is genuine because they have these details.

Be Secure

- Take the caller's number and advise them that you will call them back once you have validated their identity.
- Use a phone number from the phone book or their website, not one given to you by the caller (this could be fake). If the caller is genuine, they will understand and welcome your need to validate them.
- Don't allow yourself to be rushed. Take your time and do the relevant checks.

Tactics used by fraudsters

Persuasion

even if you are tech savvy fraudsters are smooth talkers

Urgency

vishers utilise fear tactics pressuring you into thinking you must act quickly as your money is in danger

Personal Info

can be bought from hacked company data or found on your social media/ website

Phone Spoofing

Phone numbers/IDs can be faked to hide the origin of the call

Environment

criminals can play sound effects to make it sound like they are in a call centre

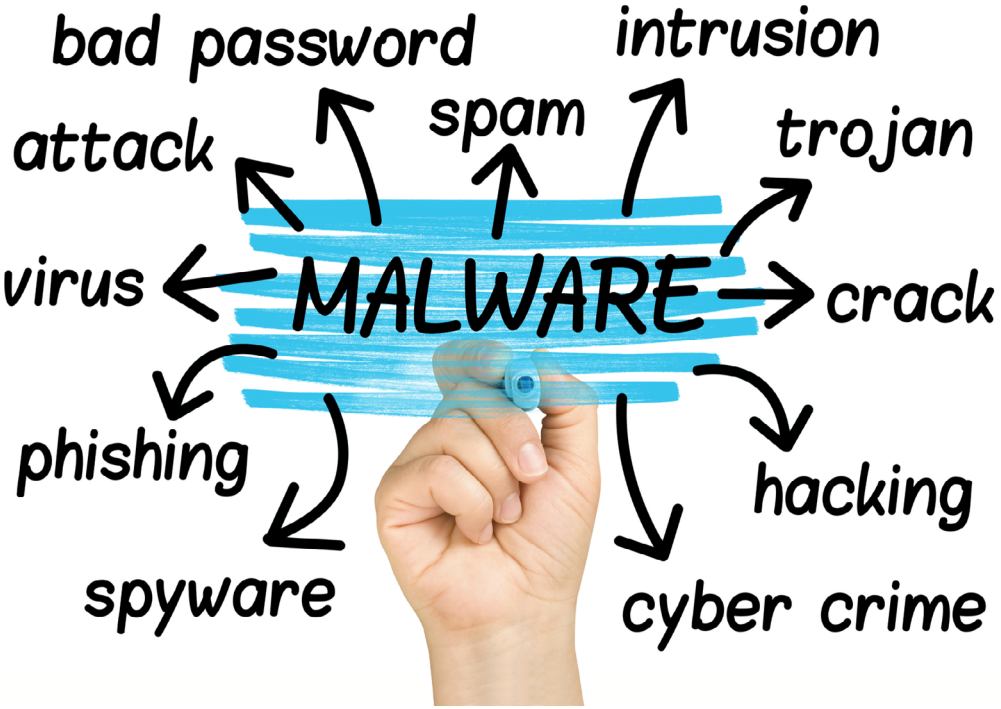
Malware

Malware is 'malicious software' designed to damage or do other unwanted actions on a computer system. Common examples include viruses, worms, Trojans, and spyware.

Cyber criminals use malware to target online bank accounts and obtain personal and financial details. It runs undetected in the background, often hidden in free software that you download from the internet or a multimedia program/file such as music or a video.

The signs to look for include:

- Advertising pop-ups (a window that opens on the screen) that appear every few seconds.
- Extra toolbars in your browser that won't go away.
- Browser going to sites you didn't tell it to.
- Unexplained system slowdowns.
- Sudden increase in computer crashes.


bad password
intrusion
attack
spam
trojan
virus
MALWARE
crack
phishing
hacking
spyware
cyber crime

Ransomware

Ransomware is a type of malicious software (malware) that encrypts the victim's data and demands a ransom in exchange for a decryption key. In simpler terms, it is like a digital kidnapping of your files.

This type of malware can be delivered to a victim's computer in many ways, such as through email attachments, malicious websites, or exploiting vulnerabilities in software. Once installed, the ransomware will begin to encrypt the victim's files, making them inaccessible without a decryption key.

After encrypting the files, the ransomware displays a message that usually includes instructions on how to pay the ransom in order to get the decryption key. The message often includes a deadline, threatening to delete the encrypted files if the ransom is not paid in time.

Paying the ransom does not guarantee that the victim will receive the decryption key or that the encrypted files will be restored. In fact, it is generally not recommended to pay the ransom as it only encourages the attackers to continue their illegal activities.

To protect against ransomware, it is important to keep software up to date, use strong passwords, be wary of suspicious emails or websites, and backup important files regularly.

Be Informed

- Ransomware can be delivered via email attachments or links. Never click on links in unsolicited emails.
- Always download mobile apps from official app stores.
- Regularly back up important files to an external hard drive or cloud storage.

Be Alert

- Don't click or reply to attachments, banners or links without knowing their true origin.
- Use unique, complex passwords for all your online accounts and avoid using the same password across multiple accounts.
- Sign up to FraudSMART alerts to learn about the latest threats and techniques used by cyber criminals.

Be Secure

- Install and regularly update reliable antivirus software to detect and remove any malware from your system. Make sure you regularly update your operating system, web browser and other software.
- Use a firewall to block unauthorised access to your computer.

What to do when you have been attacked

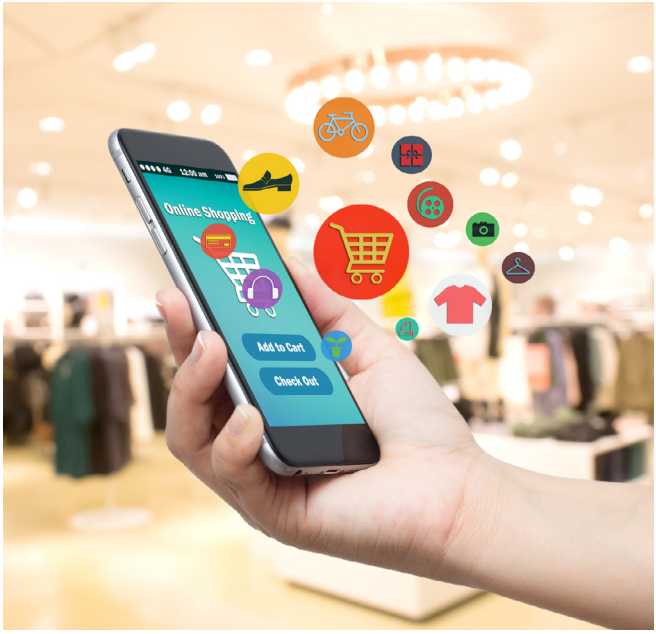
- Seek professional advice from your security service provider or if you don't have one ensure you use a trustworthy source.
- Disconnect infected computers from your business network immediately to stop the spread of infection to other computers in your network.
- Advice from law enforcement agencies is not to pay the ransom. Paying does not guarantee that your problem will be solved and that you will be able to gain access to your files again.
- Report the attack immediately to the Gardaí. The more information that you give to the authorities, the more effective they can be in disrupting the criminal infrastructure behind these scams.

Card Fraud

If you are a retailer, you probably have customers who pay remotely – either online, over the phone or by mail order.

These card-not-present (CNP) transactions, when the customer is not physically present at the time of payment, are particularly vulnerable to fraud because the buyer is 'invisible' and normal face-to-face precautions aren't possible.

There are a number of practical tools and techniques that can help keep your business safe.



Be Informed

- Ensure that you have the correct terms in place with your card processor. You must revise your terms if you are moving from solely a face-to-face business to accepting online payments.
- The card authorisation process does not guarantee payment. It only checks that there are sufficient funds in the cardholder's account and that the card hasn't been reported lost or stolen. Fraudulent payments can be reversed by the card issuer, leaving you – the retailer - out of pocket.
- Ensure all staff – including temporary and part-time - know what to watch out for.

Be Alert

- Are you selling goods that are high value and easily re-saleable? This makes them a more likely target for fraudsters.
- Be wary of unusually large bulk orders that are being delivered to residential or self-storage facilities or to countries you would not normally do business with.
- Be careful if several transactions are declined before one finally goes through.
- Watch out for a single card being used across several customer accounts or the same contact details and delivery address being used with more than one card or account.
- Always check the credentials of new customers.
- Be cautious of rush orders, especially if the customer seems unconcerned about shipping costs. Criminals often create time pressure so that you do not have time to carry out normal checks.

Be Secure

- Use 3D secure (Mastercard Identity Check and Visa Secure) and SCS/AVS (Card Security Code/Address Verification Service).
- Turn on two-factor authentication (2FA) when creating new customer accounts.
- Don't input an authorisation code given to you by the customer.
- Only make refunds to the same card used for the original purchase – and always check the card details again.

Safe Online Banking

Internet banking is a very convenient and efficient way to conduct your business banking needs, however it is vital to protect your passwords and secure log in details to prevent fraudsters gaining access to your accounts.

You or your colleagues could be tricked by phishing emails or vishing telephone calls into disclosing your password and details on fake banking websites, or to bogus callers. Fraudsters can gain access to funds either by getting you to transfer money to an account or asking you for details to allow them to make transactions themselves. They can also install malware on your system giving them access to your bank accounts and other security information stored on your computer which they can then use for identity theft.

Be Informed

- Never disclose your security details, PIN, full online banking or personal information in response to an email, phone call or letter claiming to be from your bank or other financial institution. Your bank would never ask you to disclose these.
- Your bank will never send you an email with a link to a page that asks you to enter your online banking details.
- Only ever visit your bank's website by entering the address into your browser or using a bookmark you have created using the correct address.

Be Alert

- Be aware of 'shoulder surfers' viewing your screen.
- Always check your statements, and if you notice any unusual transactions, report them immediately.
- Treat any unexpected requests to change payee or supplier's bank account details with caution. Double check the details.
- Always log out of internet banking sessions once you have finished.

Be Secure

- Never use public Wi-Fi for online banking. Use a 3G/4G connection.
- Look for 'https' at the beginning of the address and the padlock symbol in the browser frame.
- Ensure you have effective and updated antivirus/ antispyware software and firewall running before you log in to your bank account.

Cheque Fraud

Cheque fraud can occur in a number of ways. For example, a fraudster may alter a cheque, such as the payee's name or amount to be issued; create a fake cheque to steal money from a business; or steal cheques from the mail. Fraud can also occur if an employee steals cheques from their employer.

In order to prevent cheque fraud, ensure your business has proper controls in place. For example, reconcile your bank accounts regularly to identify any discrepancies. Other controls include limiting the number of employees who have access to the cheques.

Overpayment Scam

A cheque is received for payment of goods or services. The person making the payment by cheque writes it for an amount larger than they owe (i.e. they make an overpayment). They then request the business to send the overpayment back by cheque or refund to an account. This is done before the cheque clears, which is usually returned unpaid or is written from a bogus account, leaving the business with a loss.

Be Informed

- Never issue a refund of a payment, either partial or full, until you are sure the cheque has cleared fully and is not at risk of being rejected.
- When sending cheques in the post, send securely and avoid using window envelopes.
- Cross all cheques 'a/c payee only'.

Be Alert

- Ensure all issued cheques and unused cheque numbers are accounted for. Check this when you get a new cheque book and review regularly to ensure no cheques are missing.
- Always exercise caution when forming new relationships with potential customers, undertaking appropriate due diligence.

Be Secure

- Keep cheques in a secure place.
- Control who has access to cheque books.
- Do not sign cheques in advance.
- Never feel pressured into making a refund until you are sure the original funds are legitimate and secure.

Remote and Hybrid Working

As more businesses have shifted to remote and hybrid work practices, it has become increasingly important to protect your business from fraud while your staff work from home.

FraudSMARTs advice for businesses:

1. Secure your devices

- Make sure all devices used by employees for work are properly secure with up-to-date antivirus software, firewalls and encryption.

2. Establish clear policies and procedures

- Set guidelines for employees on how to handle sensitive information and financial transactions.
- Update approval procedures for payments / changes to online banking accounts.
- Review and reconcile financial reports regularly.

3. Use two factor authentication (2FA)

- Many online services or computer software programs offer two factor authentication as an extra layer of security. This means you will need to enter a code sent to your phone or email, in addition to your password to access your work accounts.

4. Limit access to sensitive

- Restrict access to only those who need it to do their jobs.

5. Conduct background checks

- Complete background checks prior to hiring new staff.
- For phone interviews, do video calls to ensure that the candidate is the same as the person who presents on the first day or follow a phone interview with an in-person interview.

6. Ensure staff are given appropriate training on cyber security with focus on phishing emails

- Phishing emails are very convincing, don't open attachments or click on links from unknown senders.

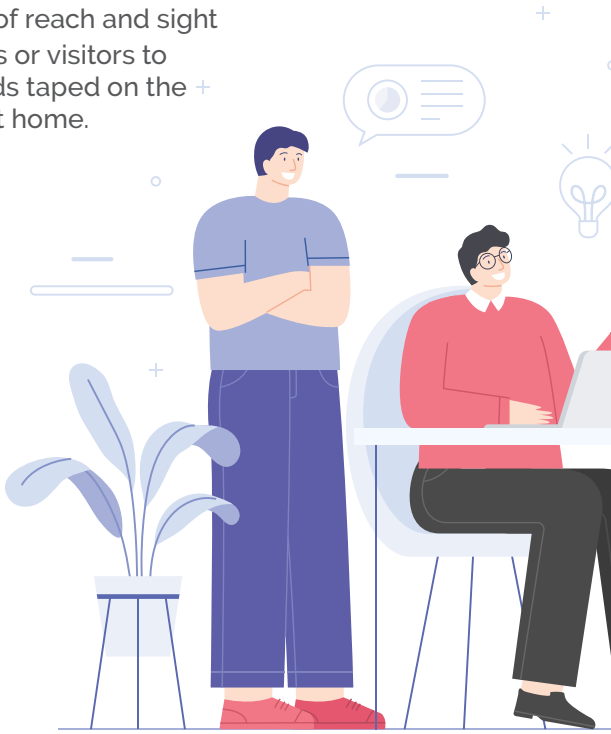
7. Remind staff, particularly those in shared accommodation, to keep passwords safe, use privacy screens if necessary and keep sensitive information private.

8. Don't allow staff to bring physical files from office to home.

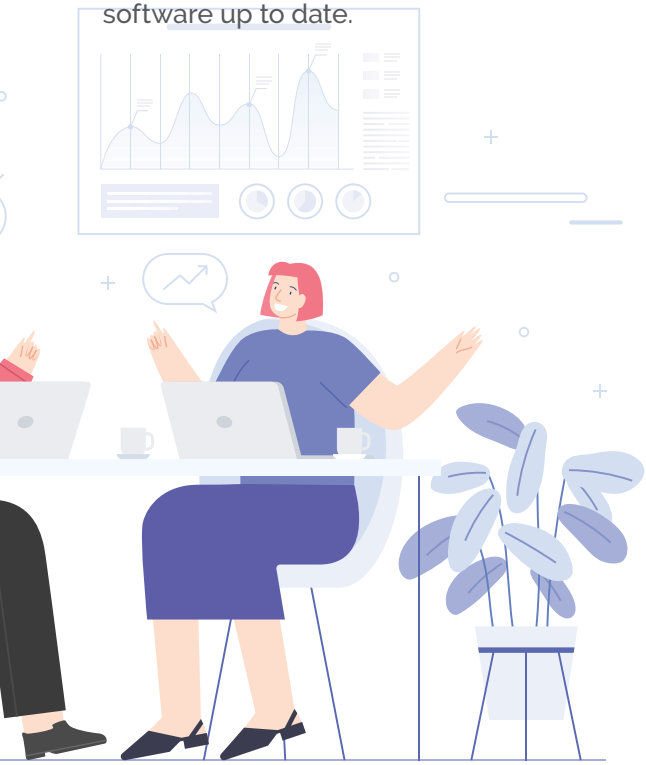
9. Be FraudSMART and sign up to receive the latest financial fraud alerts so that you can be informed of new scams and learn how to protect your business. www.fraudsmart.ie/alerts.

Advice for Employees:

1. **Keep your work devices secure:** Make sure your computer, laptop and smartphone are secured with strong passwords and updated antivirus software. Avoid using public Wi-Fi networks to connect to work devices.
2. **Keep personal and work accounts separate:** Avoid using your work email or password for personal accounts, and vice versa. This will prevent hackers from gaining access to both your personal and work information.
3. **Be careful with sensitive information:** If you are working with personal or sensitive data, be careful not to share it, even unintentionally.
4. **Keep your work area secure:** Ensure work documents and devices are out of reach and sight of family members, other tenants or visitors to your home. Don't have passwords taped on the wall or at the side of your desk at home.



5. **If you are working in a shared space:** Lock your computer when you are away from your desk.
6. **Stay up to date on company policies:** Be familiar with your company's policies on data security, remote work and fraud prevention.
7. **If you receive an email that seems unusual from a senior member in your organisation** or from a supplier with a change of bank account details for payment, contact them using a known email or phone number. Do not reply to the email or use contact details in the mail.
8. **Secure your home network:** Use strong passwords for your home Wi-Fi network and keep your router software up to date.



What to do if you are a victim of fraud?

If you suspect you have been the victim of fraud or have noticed unusual activity on your bank account(s) contact your bank immediately and also report to your local Garda Station. Fraudsters move fast; the quicker you contact your bank to safeguard your accounts the better.

A best practice guide for businesses

Protect your customers from scam messages

Commission for Communications Regulation
An Coimisiún um Rialáil Cumarsáide

These tips will help your customers identify genuine messages from you. They will also help reduce fraud on telecoms networks.

1 Keep messages to your customers simple, clear and consistent.

2 Minimise the amount of phone numbers, SenderIDs and email addresses you use to contact customers.

3 Do not ask for customers' personal details by text or email.

4 Publicise your contact details, ensure your website describes how you contact customers (e.g. phone, email, SMS SenderID) and explain how your customers can verify communications from you.

5 Make sure everyone in your supply chain is aware of and applies the information in this guide.

6 Communicate clearly to your customers how they can report scams.

7 Use hyperlinks in text messages sparingly, ensuring URLs are easy to read and understand.

8 Consider using ComReg's 'Do Not Originate' service for your inbound only phone numbers. For details see **www.comreg.ie/dno**

For additional information for you and your customers visit:
www.comreg.ie/advice-information/scam-calls/

FraudSMART

Informed. Alert. Secure.

FraudSMART was created by

Banking & Payments Federation Ireland

Banking & Payments Federation Ireland
Floor 3, One Molesworth Street,
Dublin 2, D02 RF29

Email info@fraudsmart.ie
Web www.FraudSMART.ie