POLICE SCOTLAND
Keeping people safe

Business Watch

Police Scotland Business Advice

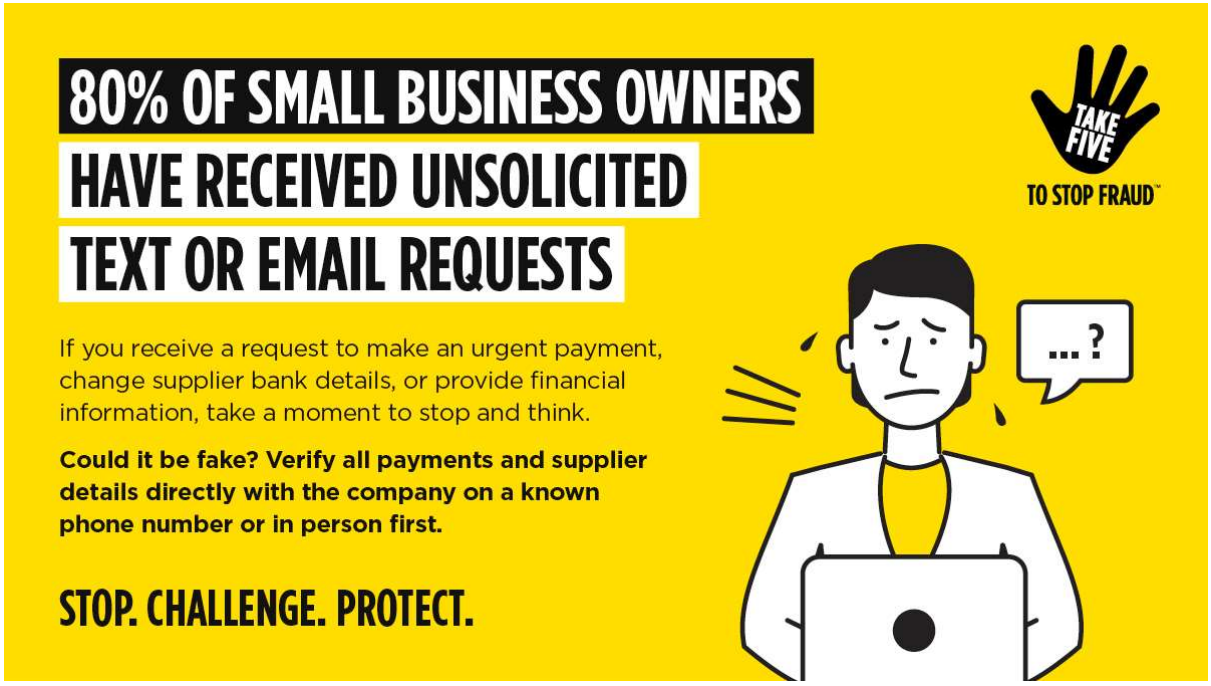
January 2022

Investment Fraud Special

Like the rest of the UK the North East has seen an increase in frauds and scams, particularly during the coronavirus pandemic, as criminals turn their attention online and to ever more sophisticated techniques to trick you into parting with your money. Being a traditionally affluent area a common victim of fraud in the North East is middle aged, with disposable income, looking for investment opportunities.

In this edition of Business Watch we detail the current top eight investment scams, highlight the criminal's tactics and give advice on how to protect yourself so you can look forward to doing business in the New Year with confidence.

Take Five to Stop Fraud – The Business Cost of Fraud



We are proud to be supporting Take Five to Stop Fraud with their campaign, The Business Cost of Fraud. In the first half of 2021 businesses saw losses of £59.2 million. Businesses are a target for criminals as their accounts will generally hold more money than the average person and some may have fewer processes and measures in place than bigger businesses.

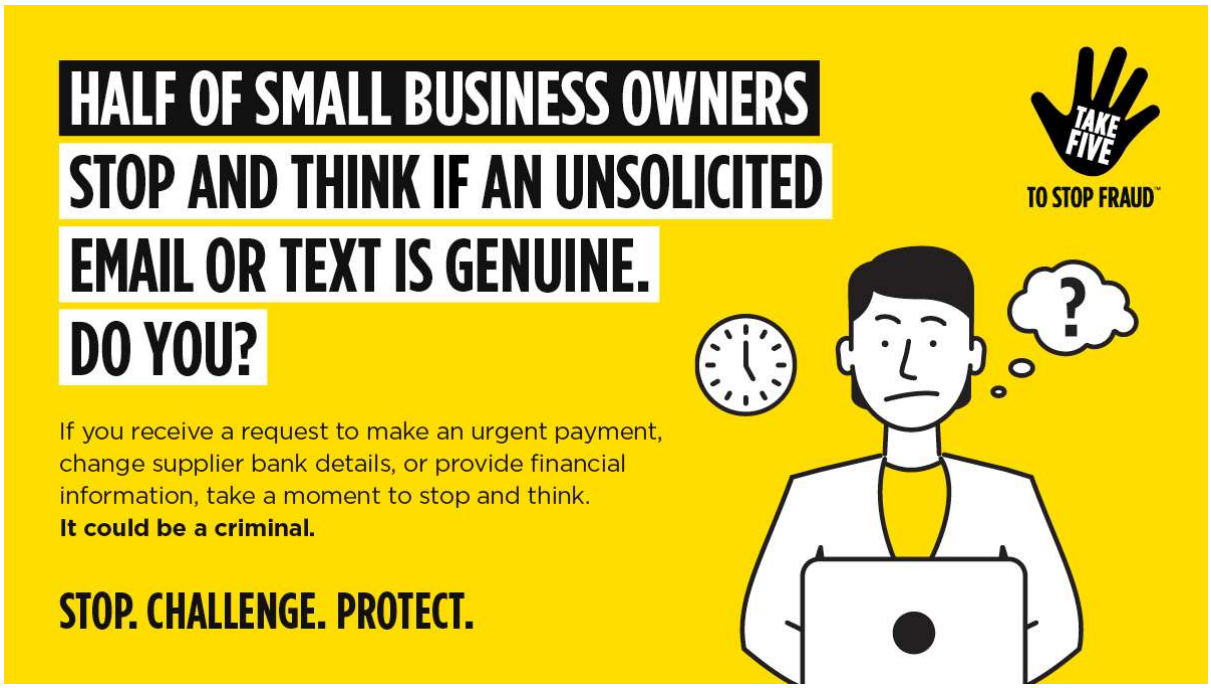
Research shows SMEs are targeted frequently by criminals, with 80% receiving unsolicited text/email requests, and 64% being targeted over the phone or in person. The impact of fraud and scams on businesses can be devastating. Many struggle to recover from the severe financial and reputational damage it can cause.

However, there are things we can all do to protect ourselves. When you're at work, if you receive an urgent request for payment or a supplier requests changes to bank details always remember to Stop, Challenge, Protect. Ask yourself if the request could be a scam? Verify the request directly on a known phone number or in person first. It may feel awkward checking with your boss but they'll be grateful that you are helping to protect the business.

In support of the campaign attached to this edition of Business Watch are a number creative assets that your company can use to promote fraud awareness among staff and clients. Consider using the Take 5 campaign graphics on email signatures and on your intranet. The full Take 5 Business Toolkit can be found at

www.takefive-stopfraud.org.uk

How do Investment Scams work?



Frauds work because on the outside they look and feel convincing and the perpetrators act and appear trustworthy. They could have the appearance of legitimate names, branding, paperwork, websites… anything you may expect to see from a genuine company, but they're fakes. They may also try and convince you they are 'experts' or have regulatory supervision when they do not.

Criminals may also claim to have lots of investors, just like you, who have chosen to take advantage of their great fund, scheme or bond. It may have published above average returns or promise to significantly increase your profits with low or very little risk. They may target you and other people in similar groups or communities (ex-pats, religious faiths, sports enthusiasts).

The tactics

- False advertising can appear on any newsfeed, search engine advertising, comparison sites (fake or genuine), and social or business media platforms. Criminals often use fake endorsements by celebrities or famous businesspeople.
- Fake websites can look professional and convincing, using official branding and logos from genuine companies. They are easy to produce and can be securely designed to prevent people finding out who really owns them.
- Mobile numbers and landlines can be made to appear as any number the criminal wants them to, including legitimate numbers for companies.
- Criminals sometimes avoid video conferencing where conversations can be recorded and people seen.
- Professional looking paperwork is available and also sent to you with in depth detail.

Access to investment portals could be provided so that you can monitor and manage the increases in your initial investment and, in many cases, an initial return on your investment is paid into your bank account. However, this is only in order to convince you to invest more. They will often encourage you to invest quickly as the offer may be time limited in some way.

How to protect yourself

Criminals are experts at impersonating people, organisations or even the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

Remember:

The best defence against social engineering attacks is knowledge. Once you know someone is trying to con you, the con will fail. Reading this article should help give you some of that knowledge.

However, even if we're suspicious, we're often bad at saying "no" to people. So, if you're uncertain, you can always try these alternatives:

"I can't make that decision without authorisation. Let me get back to you."
"I will not make any decisions without speaking to someone first."
However, don't be afraid to simply say "no" to someone.

If they're a genuine professional, they won't mind you taking the extra time to verify their identity or offer of investment. If they become pushy or insistent, then odds are fairly high that it's some form of scam.

You can also get more advice at https://takefive-stopfraud. org.uk/advice/general-advice/investment-scam/

---

1 Pension Scams

Criminals attempt to sell a too-good-to-be-true, 'one-off' investment sometimes via unsolicited contact or authentic looking websites you may find yourself. They may attempt to entice you with upfront cash payments. They often offer a 'free pension review' to give the impression that they are honest and independent advisers.

They could advise you to 'liberate' your pension into one of these schemes before you turn 55, which isn't permitted under UK pension rules and can attract an unauthorised payment tax of up to 55%.

The Scam

They may advertise online, via social media or in the small ads of reputable publications.

They design attractive offers, normally in the form of high interest rates or impossible to achieve returns, all to entice you to invest all or a substantial part of your pension pot.

They will claim they are authorised by the Financial Conduct Authority (FCA) or a similar regulator in another jurisdiction. Or, they may say they don't have to be authorised because they aren't providing advice themselves, or they're acting on behalf of the FCA or a government service.

The pension money is often invested in unusual, high risk investments, or it can be simply stolen outright.

How to protect yourself

In the UK, it is unlawful to cold call about pensions, so reject unexpected offers.

Check the status of a firm with the FCA before changing your pension arrangements. You can call the FCA helpline on 0800 111 6768 to check to see if the firm is allowed to give pension advice. You can check the authorisation status of any genuine firm on their regulator's website.

Don't be rushed into making any decision about your pension.

Be wary of promises of high returns that are 'guaranteed', 'fixed' or 'secured'. The higher the promised returns, the riskier the investment. Promises of guaranteed returns should be looked at very carefully. If it sounds too good to be true, it probably is!

Seek impartial advice and thoroughly research the company before you do anything.

---

2 The Ponzi Scheme

Criminals claim they have developed a system which is guaranteed to work. Whether it's a secret formula, or proprietary technique, it's a promised return on investment. They even have testimonials from previous customers, perhaps even people you know who vouch for it.

The Scam

There is nothing special to it. The initial investors receive a return from the money given by the second wave of investors. The second wave receive theirs from the third and so on.
You're regularly encouraged to invest additional money and to encourage as many of your friends and family to do the same, thus increasing the cost and subsequent impact of the fraud.

Some tell-tale signs include:

- The risk versus reward promises are too optimistic.
- The scheme returns don't follow overall market trends.
- The mechanics of the scheme are 'too difficult' or 'too secret' to explain.
- Reports and documentation are hard to obtain or don't have the right information.
- Depending on where the Ponzi scheme is in its lifecycle it may be difficult to remove money.
- Only select people are 'allowed' to join.
- It may be sold as a 'one-time entry' offer.
-

How to protect yourself

Look into the company offering the investment scheme thoroughly. Find as much independent information as you can by using the websites of regulators, such as the FCA. Don't trust anything you see on any website or social media to which the company directs you.

Always double check.
Choose regulated firms who have the right licences, such as the Markets in Financial Instruments Directive (MiFID) and the Insurance Distribution Directive (IDD).

Be wary of promotional material that promises great returns without much detail.

Lots of existing investors, or friends and family investing, does not mean it's not a scam. It just means there are lots of victims, some of whom you know.

Criminals will encourage you to make hurried decisions and may use technical jargon designed to baffle and confuse. They may also tell you there is a deadline in order to invest or be included due to high demand.

Ask simple questions about the company and scheme and be very wary if they dodge the questions or are unable to provide clear answers with supporting documentation.

---

3 Binary Options

Criminals claim to have a highly accessible, super easy way to gain wealth simply by betting on whether the 'option' will go up or down in value. No prior knowledge of the stock market, binary or investing is necessary, just the desire to succeed with the help of the provider.

The Scam

Like the Ponzi scheme, the fraudulent traders will tout their unique system as a way to help you beat the odds. This will be either a completely 'unfit for purpose' platform or a rigged set up which will ensure overall losses rather than gains.

To help reassure the customer a practice account – also rigged, will allow you to test the system in a safe environment using pretend money. This will deliver false successes and motivate you to spend your real money in a 'live' account.

Binary option frauds are all about manipulating an online system under the control of the scammer so it has the appearance of legitimacy and success. It is designed with the intention of the investor losing as much as possible, as quickly as possible.

How to protect yourself

From the 2nd April 2019, all firms were permanently banned from selling binary options in the UK, a similar ban enforced by ESMA (the European Securities & Markets Authority) came into force across Europe in 2018. If you are offered one, it is certainly a scam. Companies outside of Europe will also be covered by the ban, so if you are approached by a non-UK/EU firm, they are not allowed to sell these options in the UK or Europe.
If you have been a victim of a scam from before 2nd April 2019 and are in the UK, then you can contact the FCA on their consumer helpline on 0800 111 6768.

---

4 Cryptocurrency Scams

Cryptocurrency fraudsters often advertise on social media – using the images of celebrities or well-known individuals to promote and endorse cryptocurrency investments. The adverts link to professional-looking websites. Customers are persuaded to make investments with the firm using cryptocurrencies or traditional currencies.

The firms operating the scams are usually based outside the country you live in but will claim to have a local presence.

The Scam

Fraudsters will either call you or use social media platforms to advertise 'get rich quick' investments, trading in cryptocurrencies.

Criminals will convince you to sign up via cryptocurrency investment websites and to part with your personal information, such as credit card details and driving licences, to open a trading account. You're then asked to make an initial minimum deposit, after which the fraudster will call you to persuade you to invest again in order to achieve a greater profit. Even if you've realised you've been defrauded, it's usually after the website has been deactivated and the criminals can no longer be contacted.

How to protect yourself

Always be cautious if you receive uninvited investment offers, if you are pressured to invest quickly, or promised returns that sound too good to be true.

Don't assume it's real – professional-looking websites, adverts or social media posts don't always mean that an investment opportunity is genuine.

Stay in control – if you're thinking about making an investment, get independent financial advice and thoroughly research the company first.

Be wary of adverts online and on social media promising high returns on investments in cryptocurrency or crypto asset-related products.

Do further research on the product and the firm with whom you are considering investing.

Check with Companies House to see if the firm is a registered company and check for directors' names.

TAKE FIVE
TO STOP FRAUD™
STOP. CHALLENGE. PROTECT.

5 Foreign Exchange Trading

The foreign exchange market, also known as Forex, or FX, is a decentralized global market for the trading of currencies.

Criminals conduct unauthorised trading offering the chance to trade in the foreign exchange. They often use posts on social media which contain fake celebrity endorsements and images of luxury items. The posts link to websites created by criminals that have the look and feel of a real Forex trading platform. Offering guaranteed profits, they create accounts for you, with some receiving small returns to portray legitimacy, which in turn gives you the confidence to trade further.

The Scam

The trading account that you're given access to may appear real, however it's a manipulated demo account where no actual trades take place.

You may be deceived into thinking that your investment has made a profit and you may even receive a small return.
You're then encouraged to invest more money (for greater profits) or introduce others to the fake platform and if you want to withdraw, you'll be charged exit fees. Eventually the returns stop, and your account is closed with no further contact.

How to protect yourself

Be suspicious of any approaches or adverts on social media. Do not give out personal or financial details.

Never agree to anything or send money upfront, without making your own enquires into the company or individual first.

Don't assume it's real. Professional looking websites, adverts or social media posts don't always mean that an investment opportunity is genuine. Criminals can use the names of well-known brands or individuals to make their scams appear legitimate.

Stay in control. If you're thinking about making an investment, thoroughly research the company first and consider getting independent advice.

Make the right checks, firms providing regulated financial services must be authorised by the FCA. You can check whether they are authorised on the Financial Services Register section of the FCA website. Use the contact details on the register, not the details the firm gives you, to avoid possible 'clones.'

TAKE FIVE TO STOP FRAUD

6 Overseas Property and Cropscams

Fraudsters may offer you the chance to buy a plot of land, for example, a plot on a plantation that harvests agricultural commodities such as teak trees, jatropha, paulownia and biofuels.

The investment is usually stated to be low risk but promising high, often guaranteed returns of around 15–25%.

The investment period is typically about five years, after which your plot will be harvested and sold on your behalf and the profits forwarded to you.

The Scam

Criminals usually call individuals out of the blue, but can also make contact via email, post or word of mouth.

They can also target you at an event, seminar or exhibition. They may use professional looking material including brochures, websites and videos to convince you that their property or crop investment is a great opportunity. Once investment is made the criminal may then cut contact straight away or try to get more money from you first.

Regardless, either the land doesn't exist, or the criminal has no rights to sell it.

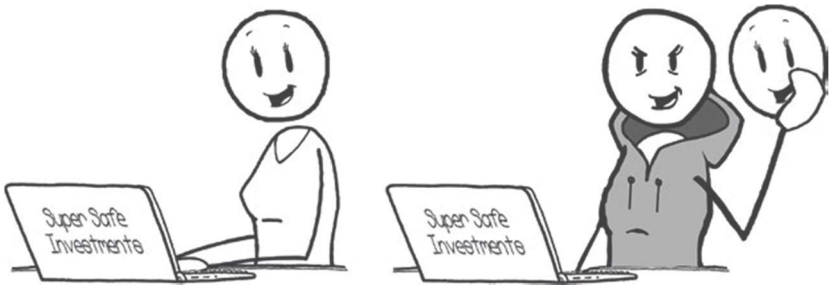
How to protect yourself

If it sounds too good to be true, it probably is.

Genuine land and property companies will most likely make their offering via a network of independent financial advisers and brokers and via advertising rather than contacting you by phone. Be wary of someone calling you to directly offer you a plot of land.

Research both what you have been offered, and the investment company. Speak to Trading Standards if you have concerns.
Consider getting impartial information and advice from registered financial institutions and brokers.

The FCA does not regulate the sale of land, trees or crops, nor do the regulators in other countries and jurisdictions. However, they do regulate Collective Investment Schemes (CIS) which can involve overseas property and crop schemes.



7 Unregulated Investment Scams

A Collective Investment Scheme (CIS) is a pooled investment that usually has several people contributing to it and is invested by a fund manager into one or more types of assets.

An Unregulated Collective Investment Scheme (UCIS) is one that is neither authorised or recognised by the FCA and as such are not subject to UK requirements, making them riskier assets (forestry, property, film production) or investment strategies (compared with CIS). The FCA may have a register you can check to determine if a CIS is authorised or unregulated.

The Scam

Some UCIS are just straightforward scams. Some are genuine, but can in many cases over-promise and under-deliver, or are sold illegally.

Usually they claim to offer high returns, which you should always see as a red flag. High returns always come with high risk.

Scams are often based outside of the country in which you reside but claim to have a local base, often a prestigious London address.

How to protect yourself

Always be cautious if you receive any uninvited investment offers, if you are pressured to invest quickly, or promised returns that sound too good to be true.

Check the FCA website to make sure you're not dealing with a known scam.

Check Companies House to see if the company is registered in the UK or the local commercial registers if outside the UK and look for the names of directors – many have a chequered past and there may be information about them online.

Check investment web forums – people often post concerns about firms or investments. Always seek independent financial advice or guidance before investing.

Because they're unregulated, you can't make a complaint to the FCA, if you think you were mis-sold the product or caught by a scam. The Financial Services Compensation Scheme (FSCS) may provide protection if an authorised firm which you have been dealing with has done something wrong and goes out of business. The Financial Ombudsman Service settles complaints about authorised financial services firms.

If you use the services of a firm that is not authorised you generally will not have access to the FSCS or the Ombudsman.

---

8 Clone Firm Scams

You find yourself, or are approached by, an investment firm which claims to be registered with the FCA. Once contact has been made, and 'bona fides' established, then the criminal can attempt to run any of the other types of Investment Scams in this article, or indeed any type of fraud.

The Scam

Criminals set up fake firms, but use the name, address and Firm Reference Number (FRN) of genuine investment companies registered with the FCA. These might include websites with a slight difference in the URL. They may use the correct reference numbers on the FCA website and may even fake up official looking logos or kite marks. Once set up, these fraudsters will then send sales materials either linking to their doctored website, or the websites of legitimate firms, to dupe you into thinking they are the real firm when they are not. They can then run whatever scam they choose once they have convinced you of their authenticity.

How to protect yourself

Reject unsolicited investment offers whether made online, on social media or over the phone. Be wary even if you initiated contact.

Always check the FCA Register to make sure you're dealing with an authorised firm and check the FCA Warning List of firms to avoid.

Only use the telephone number and email address on the FCA Register, not the contact details the firm gives you.

Look out for subtle differences in URLs, email addresses, phone numbers and the FRN number. Don't forget that incoming phone numbers can be spoofed or disguised.

Consider seeking impartial advice before investing.

Get help and report a scam

If you think you have uncovered a scam, have been targeted by a scam or fallen for a scam, there are many authorities you can contact for advice or to make a report.

In the first instance, you should contact your bank immediately on a number you know to be correct, such as the one listed on your statement, their website or on the back of your debit or credit card.

Report to Police Scotland directly by calling 101 or Advice Direct Scotland on 0808 164 6400.

Every report assists police investigations, provides intelligence, informs national alerts that protect all communities, disrupts criminals and reduces harm.

In the UK you can forward scam text message to OFCOM on 7726 (free of charge), and forward suspicious emails to report@phishing.gov.uk

And don't forget to share your experience with friends and family to make sure they don't fall for the same scam.

Financial Conduct Authority (FCA)

In the UK, a firm must be authorised and regulated by the Financial Conduct Authority (FCA) to do most financial services activities.

Financial Conduct Authority (FCA) www.fca.org.uk or 0800 111 6768
www.fca.org.uk/scamsmart

Financial Service Compensation Scheme (FSCS)

www.fscs.org.uk

Financial Ombudsman Service

www.financial-ombudsman.org.uk

National Trading Standards

www.nationaltradingstandards.uk/work-areas/scams-team/

Scottish Business Resilience Centre App Launched

Reminder that recently the SBRC launched a new app to provide advice and support for businesses to do everything they can to stay safe – online and offline. Through targeted push notifications, businesses that download the app will be informed of credible threats to their operations including cyber threats, traffic, and protestor activity, and be given accurate sector-specific guidance within minutes.

https://www.sbrcentre.co.uk/scottish-business-resilience-centre-app-launched

---

TRADING STANDARDS SCOTLAND BULLETIN

Business advice and Scam Bulletins from Trading Standards Scotland can be found at

https://www.tsscot.co.uk

Aberdeenshire Trading Standard Bulletins can be found on the following link

http://publications.aberdeenshire.gov.uk/dataset/trading-standards-crime-and-scams-bulletin

Sign Up for Neighbourhood Alert for free

A great way in which Police can share information is via the Neighbourhood Alert system, which is delivered by Neighbourhood Watch Scotland. This enables us to send out e-mail messages relating to local crime trends and share crime prevention advice quickly and effectively to a wide audience. The information can also be targeted to particular groups, streets, or communities as required.

Anyone can sign-up to receive these e-mail messages, either individually or as a community group. The sign-up process allows you to specify the type of information you are interested in and from what source. This is coordinated by our partners in Neighbourhood Watch Scotland, who work with a range of partners in the public sector to provide information not only on crime, but also about community safety and resilience. We only send out messages which contribute to keeping you informed and safe.

Simply visit
www.neighbourhoodwatchscotland.co.uk

Crimestoppers - https://crimestoppers-uk.org/

Tel. 0800 555 111

SPEAK UP. STAY SAFE - CRIMESTOPPERS are an independent charity that gives people the power to speak up to stop crime 100% anonymously.

ARE YOU READY FOR A LIFE CHANGING CAREER? -
http://www.scotland.police.uk/recruitment/police-officers/

As always please share the above information with your colleagues.

Should this bulletin be sent to one of your colleagues as well as you? If you are 'moving on' please let us know a new contact within your company to send the bulletin to.

If you have any sister companies or businesses you work closely with who you think would benefit from this bulletin (check with them first) then please let us know.

If you no longer wish to receive this bulletin then please let us know at NorthEastCrimeReduction@Scotland.pnn.police.uk

URGENT MESSAGES WILL BE SENT OUT AS APPROPRIATE

Crime Reduction Unit
North East Division

Email: NorthEastCrimeReduction@scotland.pnn.police.uk
Website: www.scotland.police.uk
Twitter: www.twitter.com/NorthEPolice
Facebook: www.facebook.com/NorthEastPoliceDivision

Police Scotland's North East Division covers rural and urban areas in Moray, Aberdeenshire and Aberdeen City. The division has five territorial command areas which have their own dedicated Area Commander, who is responsible for the daily policing function. Each command area is served by a number of community policing teams whose activities are built around the needs of the local community. These teams respond to local calls and look for long term solutions to key issues. They are assisted by the division's Crime Reduction Unit who deliver against Force and local priorities in a number of areas, including physical and social crime prevention, supporting and enhancing community engagement and creating and sustaining strong and effective partnership working