Company and director sentenced after carrying out unregistered gas work

A Chelmsford based company and director have been fined after conducting gas work at a domestic property in Mount Pleasant, Maldon without being gas safe registered.

Chelmsford Crown Court heard how N Murray and Sons Ltd had been contracted in May 2014 to install two boilers at two domestic properties in Essex. Following the boilers being fitted complaints were made to Gas Safe register.

Gas Safe Register inspectors subsequently confirmed that the gas appliances installed by an employee of N Murray and Sons were considered to be “at risk” and required immediate work to ensure the safety of the occupiers of the properties.

An investigation by the Health and Safety Executive (HSE) found that Nigel Murray, director of N Murray and Sons Ltd, had sub contracted gas installation work to his son who he knew was not Gas Safe Registered. It was also found that Nigel Murray was aware that Grant Murray was not competent or gas safe registered but allowed the work to be completed.

N Murray and Sons Ltd of Chelmsford pleaded guilty to breaching two charges of Regulation 3 (2) of the Gas Safety (Installation and Use) Regulations 1998.

The company has been fined £6000.

Nigel Murray pleaded guilty to breaching two charges of Section 37 of the Health and Safety at Work etc Act 1974 and has been sentenced to a six-month community order and a 7pm – 5am curfew for four months.

Grant Murray pleaded guilty to breaching two charges of Regulation 3 (1) of the Gas Safety (Installation and Use) Regulations 1998 and he has been sentenced to a 12-month community order and a 7pm – 5am curfew for six months.

Speaking after the hearing HSE inspector Edward Crick said: “Gas Safe Registered engineers are regulated and have to ensure they can prove they are competent. This safe guard is removed when people choose not to register which is highlighted in this case, where the individual placed people at risk of harm in their homes.

“It is important that anybody who has gas work carried out checks their engineer is carrying a valid gas safe registered identification card. They should also check online or call Gas Safe Register to confirm they are competent to carry out the work.”

Notes to Editors:

1. The Health and Safety Executive (HSE) is Britain's national regulator for workplace health and safety. We prevent work-related death, injury and ill health through regulatory actions that range from influencing behaviours across whole industry sectors through to targeted interventions on individual businesses. These activities are supported by globally recognised scientific expertise. www.hse.gov.uk
2. More about the legislation referred to in this case can be found at: www.legislation.gov.uk/
3. HSE news releases are available at http://press.hse.gov.uk

Journalists should approach HSE press office with any queries on regional press releases.

Benoît Cœuré: A Euro Cyber Resilience Board for pan-European Financial Infrastructures

Introductory remarks by Benoît Cœuré, Member of the Executive Board of the ECB, at the first meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt, 9 March 2018

It is a pleasure to welcome you back to Frankfurt. Our last meeting was in June last year. Today, we will discuss the future course of the high-level cyber resilience forum for pan-European financial market infrastructures, critical service providers and competent authorities.

Establishment of the Euro Cyber Resilience Board for pan-European Financial Infrastructures

Recent technological advances have enabled cybercriminals to conduct ever more sophisticated, precise and powerful attacks. And nobody is immune to cyber risks, including businesses, financial infrastructures and public administrations. So we should avoid a "blame and shame" culture and work together.

The ECB and the Eurosystem are striving to lead by example. At the ECB, overseers, operators, supervisors and IT security services are working together more closely on cyber issues. Within the Eurosystem, there has been close collaboration on implementing the Eurosystem oversight cyber resilience strategy for financial market infrastructures that we presented at our last

meeting, in line with CPMI-IOSCO's guidance on this topic.[1] The Market Infrastructure Board, which is in charge of Eurosystem financial market infrastructures, has also scaled up its activities to ensure the continued cyber resilience of its systems and platforms.

Eurosystem initiatives are part of a growing international effort to combat cyber threats. The CPMI-IOSCO guidance is being implemented. In October 2017, the Financial Stability Board (FSB) delivered a stocktake report of relevant regulations and supervisory practices to G20 finance ministers and governors, and G7 ministers and governors published the "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector".[2] The FSB will produce a common lexicon of important terms, while the G7 Cyber Expert Group continues to work on third-party risks, cross-sector coordination and threat-led penetration testing, and will make proposals for G7 cross-border cyber crisis simulation exercises.

In this context, the Eurosystem aims at coordinating its own activities in the field of cyber risks with that of market participants and other public authorities to succeed in protecting the financial system from cyber threats. I therefore invite you today to become part of the Euro Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures – a regular forum where we can work together in a trusted environment.

The ECRB's objective is to enhance the cyber resilience of financial market infrastructures and their critical service providers, as well as that of the wider EU financial sector, in line with international standards. This will be achieved by fostering trust and collaboration and facilitating joint initiatives – whether among market players or between market players and authorities. The ECRB will thus contribute to the overall stability of the EU financial system.

The ECRB will have no formal powers to impose binding measures and will not make supervisory judgements. Its legitimacy will stem from the voluntary commitment of its members to abide by its common positions, statements and strategic views.

The ECRB will be chaired by the ECB, which will be closely involved together with national central banks and observers from the relevant European public authorities. This will ensure that the ECRB acts in the interest of Europe as a whole. Its common positions, statements and strategic views will be adopted by consensus.

To kick off the work of the ECRB, we would like to reflect with you on possible work items which we could address collectively. As part of this, we will also report on two of our most recent activities.

First, a cyber resilience survey, developed under the Eurosystem oversight cyber resilience strategy, was conducted across more than 75 payment systems, central securities depositories and central counterparties throughout Europe. As you will see, the survey highlighted a number of very pertinent issues for discussion, such as cyber governance, training and awareness, and cyber incident response.

Second, the Eurosystem is currently finalising the main elements of the European Threat Intelligence-Based Ethical Red-Teaming (TIBER-EU) Framework. This is an interesting concept which we hope will raise the level of cyber resilience in Europe and enable cross-border, cross-authority testing, which has not been done before.

We look forward to hearing your feedback on these two initiatives. We will also update you on the forthcoming market-wide exercise, which will explore the challenges of a specific cyber scenario and see how we can work closer together in times of crisis.

I am confident that we will have a fruitful discussion. I will now hand over to my colleague Sabine Lautenschläger, who will make some introductory remarks from the supervisory perspective.

After that, I would like to invite the European Commission representative to briefly introduce the very recently published "FinTech Action plan", which presents some interesting points to be considered with regard to the cyber resilience of the financial sector.

Thank you.

Sabine Lautenschläger: Cyber resilience – objectives and tools

In 1903, the Italian inventor Marconi demonstrated his new invention, a wireless telegraph, to a large audience. It didn't go too well for him, though. The machine itself did work in the sense that it transmitted a message. However, it was not the message the audience – or Marconi – had expected. The word "rats" was being sent again and again. The system had been hacked. The culprit in this case was Nevil Maskelyne, a magician. Allegedly, he had been hired by a British wired-telegraph company which was worried that Marconi's invention might ruin its business.

Technology has advanced a lot since 1903. And it has created a deeply interconnected world. The financial system is a case in point. No financial institution can survive, let alone thrive, on its own. No bank can do without the complex web of financial market infrastructures that underpins its day-to-day business. No bank, therefore, must underestimate the associated risks. In particular, no bank must underestimate the IT risks, which include cyber risks. In the worst case, a single hack could compromise the entire system. So cyber resilience is a goal we all share. And anyone who sees it as just another competitive advantage is mistaken; the whole chain is only as strong as its weakest link. And in that sense, many actors in the financial system are parts of the same chain.

ECB Banking Supervision takes cyber resilience very seriously. Naturally, we focus on banks and on the euro area. In doing so, we take into account that banks are not just connected among themselves but also with other market participants and infrastructures. This means that our supervision of IT risks also covers the end-points of payment systems and market infrastructures in the banks directly supervised by us. In short, we aim to ensure the availability, confidentiality and integrity of banks' data and systems.

What have we done so far and what are our plans for the future?

- So far, we have conducted thematic reviews on cyber risk and outsourcing. One result is stating the obvious: there is some concentration in terms of companies to which banks outsource IT functions. Apart from concrete bank-specific findings, the reviews have helped us to get a better idea of the risks. And they have made banks more aware of them.
- We have conducted a stocktake on how IT risks are supervised outside the euro area. This helped us to identify best practices; and it will help us to define our own supervisory expectations. Work is ongoing as part of our contribution to the work programme of the European Banking Authority, the EBA.
- We have conducted quite a few on-site inspections into IT and cyber risks, using state-of-the-art methods. Looking ahead, our aim would be to have such inspections every three or four years for large banks.
- We have set up a reporting framework for cyber incidents. Since mid-2017, banks have been required to report significant cyber incidents. This will help us to quickly react in a crisis and make us aware of common vulnerabilities.

Drawing on guidelines from the EBA, we have developed comprehensive IT risk self-assessments for the banks we supervise, including an extensive section on IT and cyber security. The results of these assessments will feed into our Supervisory Review and Evaluation Process, in which we will also challenge the information provided by banks. We will do so as a result of our insights from on-site inspections and from reports of cyber incidents. The information collected will then serve as a basis for a thematic review of IT risks. This review will give us a better idea of the overall IT risk landscape in the banking industry. It will allow us to identify blind spots early on and define areas which we need to investigate further; this will eventually feed into our plans for 2019. In addition, the review will also help us to compare banks. Partially anonymised feedback could then be shared with them.

Ladies and gentlemen, there is one thing we need to keep in mind. Right from the start, hacks gained a lot of attention, while preventing them did not. In finance, as in many other fields, it is mostly just mundane work that helps to keep things safe. I wonder whether cyber risk is as unique as we are inclined to believe. I have no doubt that we need to take it seriously and that we need to work towards making banks more resilient. In doing so, we should also welcome new ways of tackling cyber risk, of course. But this I would like to do within the existing framework of banks' risk management. Cyber risk needs to be part of general risk management procedures, of general crisis management, and general business continuity planning. After all, it is

an operational risk. And our experience in dealing with operational risks can help us to cope with cyber risk as well.

We must keep in mind that cyber risk does not invariably arise from the technology itself but also from how we use it. It is people who are behind the hacking. And often, it is people who leave doors unlocked and gates wide open for cyber criminals to sneak in. People play a big role when it comes to cyber resilience. Thus, it makes sense to draw on the principles we have established for risk management and governance, and on the experience we have gained in these areas.

Ladies and gentlemen, I am aware that this kind of work is unlikely to capture the public's attention in the same way as Mr Maskelyne did in 1903. But it needs to be done. While cybercrime may have an aura of mystery and power, cyber resilience is quite the opposite: it calls for vigilance and diligence, day in, day out.

Thank you.

Press release: Waste vehicle seized from gang

A vehicle belonging to an organised gang operating in South East England has been seized by the Environment Agency and Thames Valley Police, as part of an ongoing waste crime investigation. The vehicle is believed to be linked to the operation of an illegal waste site in the Maidenhead area.

The seizure, which took place last week, comes as the Environment Agency and the police move forward in their investigation to capture those responsible for occupying land unlawfully and accepting tonnes of waste, often from unsuspecting sources, leaving behind the rubbish to be cleared at the expense of the landowner or taxpayer.

Illegal waste crime drains the UK economy of £1 billion each year in clean-up costs and lost tax revenues. It has a devastating effect on the environment and local communities with pest infestations and fires, which could lead to water and land contamination plus air pollution from smoke.

Nick Daykin, Environment Agency Enforcement Team Leader, said:

> This is a great result in an ongoing investigation with Thames Valley Police to apprehend a group of unscrupulous individuals. The power to seize vehicles is a relatively new and is now an important weapon in our armoury for disrupting this type of criminal activity. This is a big message to the criminal fraternity: you set

> up site yesterday, we will have one of your vehicles off the road today and we will do it again tomorrow!
>
> Using illegal waste dealers may seem tempting in terms of cost, but it can help fund organised crime. Everyone has a responsibility for their own waste and if your waste is found at an illegal site you could be facing fines of up to £5,000. To avoid this, we encourage members of the public and local businesses to ask their waste carrier for proof of their Waste Carrier's Registration and to ask to see a 'waste transfer note' and if possible take a photo of it on their phone.

Contact

All press enquiries: 0800 141 2743

Press release: Waste vehicle seized from gang

A vehicle belonging to an organised gang operating in South East England has been seized by the Environment Agency and Thames Valley Police, as part of an ongoing waste crime investigation. The vehicle is believed to be linked to the operation of an illegal waste site in the Maidenhead area.

The seizure, which took place last week, comes as the Environment Agency and the police move forward in their investigation to capture those responsible for occupying land unlawfully and accepting tonnes of waste, often from unsuspecting sources, leaving behind the rubbish to be cleared at the expense of the landowner or taxpayer.

Illegal waste crime drains the UK economy of £1 billion each year in clean-up costs and lost tax revenues. It has a devastating effect on the environment and local communities with pest infestations and fires, which could lead to water and land contamination plus air pollution from smoke.

Nick Daykin, Environment Agency Enforcement Team Leader, said:

> This is a great result in an ongoing investigation with Thames Valley Police to apprehend a group of unscrupulous individuals. The power to seize vehicles is a relatively new and is now an important weapon in our armoury for disrupting this type of criminal activity. This is a big message to the criminal fraternity: you set up site yesterday, we will have one of your vehicles off the road today and we will do it again tomorrow!

> Using illegal waste dealers may seem tempting in terms of cost, but it can help fund organised crime. Everyone has a responsibility for their own waste and if your waste is found at an illegal site you could be facing fines of up to £5,000. To avoid this, we encourage members of the public and local businesses to ask their waste carrier for proof of their Waste Carrier’s Registration and to ask to see a ‘waste transfer note’ and if possible take a photo of it on their phone.

Contact

All press enquiries: 0800 141 2743