EIG

Financial Crime Checklist

	Yes/No	Action
Proceeds of Crime Do your policies and procedures take account of your legal obligations under the following legislation: Proceeds of Crime Act, Money Laundering Regulations 2007, Terrorism Act and Bribery Act 2010? Is there a designated Compliance Officer and/or MLRO?		
Sanctions Do you screen your customer list, employees, third parties and new directors against the HMT Sanctions list? Do you have a procedure in place for dealing with 'hits' identified on the HMT Sanctions list?		
NCA Do you have a process in place for investigating suspicious activity and reporting to NCA? Are you and your staff (where applicable) aware of your responsibility to identify suspicious activity and escalate to the designated person?		

Staff training Is financial crime training provided to all members of staff, and has it been tailored to the requirements of their job? Does this training include a test? Is financial crime training repeated at regular intervals (at least every two years)? Is the financial crime knowledge of key members of staff regularly updated?		
Data Security Is there a specific focus on data security in your firm? Is there a specific individual with responsibility for data security? Do you have any written policies or procedures covering data security which are proportionate to your business? Does the culture of the firm encourage staff to report data security concerns? **Access to systems** Are recruitment processes robust enough to identify potential staffing issues or concerns? Do staff have appropriate access to customer data in their day to day role? When staff change roles are unnecessary access rights removed in good time? Could you perform random checking to ensure that staff are accessing customer data for legitimate business reasons? **Outsourcing**		

How well do you know your third party suppliers or service providers? Have you carried out any due diligence on third parties, including their security arrangements and staff recruitment policies? Do you allow third parties unsupervised access to your office or records? Do you maintain a clear desk policy to reduce the risk of customer data being lost, stolen or becoming accessible to unauthorised persons? **Physical control** Do you allow staff to work remotely or take customer data outside the office on laptops, or other portable devices? If so, are the data files or the devices themselves encrypted? Do you monitor the content of laptops or portable devices? Would you know if laptops or portable devices were to go missing? Are you satisfied with the consistency and security of the backup of your data? Have you identified any vulnerability in the security of or access to your premises? **Disposal of data** Do you shred your customer data in house and if so, are staff aware of the		

requirements? If you use a third party for disposal of data, are you satisfied with their security and staff vetting arrangements? If you have ever disposed of a computer, did you wipe the hard drive with specialist software or remove and destroy the hard drive? **Data compromise incidents** Do you have a designated individual responsible for data security incidents? Would your staff recognise a data security incident and how to report it?		
Fraud What are the main fraud risks in your business? Have you considered fraud risks arising from products, distribution channels, staff and services to customers? How do you measure fraud loss? Is fraud loss measured consistently across the business and not hidden within other costs such as bad debts and insurance claims? **Insurance fraud** Which insurance products pose the greatest risk to your business? How do you monitor suspicious claims? **Staff / Internal fraud** Do you have tailored fraud awareness training in place for your staff? Are your employees monitored for their		

performance against fraud management indicators and is it monitored and action taken where it falls below accepted standards? Are you producing newsletters or other alerts to inform staff about fraud risks and trends? Are new recruits in high-risk positions (e.g. finance department) subject to enhanced vetting (e.g. criminal records checks)?		
Anti-bribery and Corruption Have you undertaken a review of the risks posed to your business? Has your review covered: • Governance and management information; • Risk assessment and responses to significant events; • Due diligence on third party relationships; • Payment controls; • Staff recruitment and vetting; • Training and awareness; • Remuneration structures and associated risks; • Incident reporting; and • Role of compliance and internal audit.		