

## **5 ways to stop ID Theft at work**

Identity theft at work puts the livelihoods of the owners and the jobs of 12 million employees at serious risk. Criminals frequently target businesses for sensitive information as it is often easier to get hold of that data than from people's homes. Companies have an important responsibility to protect and correctly dispose of the confidential information held on their staff and customers.

There are various ways you can protect yourself and those who work with you from identity theft. Just follow these 5 simple tips:

### **1. Shred sensitive information**

Always shred confidential information. To be on the safe side – shred everything. A reputable shredding company will safely and securely destroy your paperwork beyond recognition for just a few £pounds and recycle the waste for you too. For extra peace of mind they can do it on site quickly in mobile shredding units. Thieves raid rubbish bins – don't leave it to chance.

### **2. Use lockable bins and tamper-proof sacks**

Identity theft isn't always carried out by an unknown criminal. In many cases it is found to be carried out by staff or ex-employees. Protect yourself from internal fraud by using lockable bins and tamper-proof sacks for all confidential information. Entrust responsibility to select personnel and use a BSIA accredited shredding company to collect and dispose of the waste.

### **3. Check your post**

Have you noticed post has been going missing? Has the bank sent you documents you never received? Did a client complain you hadn't replied to a letter? If you suspect post is being intercepted tell the Post Office (and the manager of the building) immediately.

Make sure you tell everyone your new address as soon as possible – preferably before you leave. Don't assume post from your old address will be forwarded on. To be extra safe, use the Royal Mail's Redirection Service for 6-12 months.

### **4. Don't give confidential information to unknown callers or mailers.**

Make sure your company policy clearly states that employees must not divulge sensitive information to unknown callers or e-mailers.

Be selective in who has access to confidential data and monitor all release of information on staff, clients and financials. Never write down account numbers, pins or bank details.

### **5. Don't risk important documents**

Be vigilant when taking financial details to meetings or the bank. Minimise the need for carrying sensitive information around and make sure there are always two people transporting cash or data. Password protect confidential information held on the computer and restrict access to classified reports that are e-mailed. Make sure you have the necessary protection in place when dealing with or receiving online transactions. Upgrade your firewall and security software frequently.

**Shred Secure are a BSIA approved shredding company and can safely and securely dispose of paper and disks. For more information, contact their friendly team on 01908 562504.**