

One of the greatest data security threats is from agents and staff

but so far none have publicly admitted to doing so. However, Sapna Capoor, global biometrics analyst at consulting firm Frost & Sullivan, agrees that the time is right for the call centre industry to embrace the technology. She says: "A growing number of transactions are occurring over the telephone, and fraud is becoming an ever-higher cost. Biometrics is expensive, but we're reaching the point where it is a worthwhile investment for many call centres."

As the HSBC example illustrates, one of the greatest threats to data security comes from call centre agents themselves. The industry has a staff turnover rate of higher than 20 per cent and many firms employ temporary staff during seasonal peaks. The opportunity and the temptation for an employee to steal customer data can be great.

Some centres choose to tackle the risk using technology. Tim Morgan, chief technology officer at speech technology solutions provider VoxGen, says: "When the Inland Revenue was asking business owners to deliver their self-assessment tax returns by telephone, we helped them to remove the agent from the identification process. We used a voice recognition system to verify the identity of callers. This meant that agents had no access to sensitive customer data. As an added benefit, the Inland Revenue needed to employ fewer agents."

24/7 Customer, a call centre company with operations in India, The Philippines, Guatemala, and Belfast, tackles the problem by closely controlling the activities of its 6,500 agents. "We have extensive CCTV coverage of our call centres," explains Hariharan Sundaram. "We don't allow mobile phones. No one is allowed to take paper out of the buildings. We only give agents access to dumbed-down terminals that have no functioning USB ports."

However, Aurea Fellows, managing consultant at business psychology firm, Kaisen Consulting, believes that the best way for call centres to stop agents stealing customer data is to stop those agents leaving. However, she believes that tackling staff turnover will require a major shift in recruitment policies: "Call centres tend to hire young, ambitious people, and then find that these are precisely the sort of people who tend to be bored by a job that involves reading from scripts and following rigid procedures. Those people become dissatisfied, and leave."

She continues: "Sky and William Hill were able to reduce staff turnover by 50 per cent simply by recruiting on motivation rather than capability. In interviews they looked at how people said things, as well as what they said. They looked for people who would have a good lifestyle fit with a call centre,



Fingerprint file: High-risk data security sites frequently require fingerprint access

such as young mothers and more mature workers."

It's not only call centres that can lose customer data. It can be lost at the back-end just as easily. In fact, a recent survey amongst 227 information security professionals found that a shocking 49 per cent do not employ firewalls, the most basic level of security against unauthorised access to sensitive information. However, there is still much more that call centres can be doing to protect consumer data. As fraud becomes ever more prevalent, and security measures become ever more affordable and usable, we can expect to see a growing number of call centres beginning to use them. ■