Market Conditions

Halfway through 2010 it has become abundantly clear that conditions for buyers of financial institutions insurance have eased considerably from those of 2008 and 2009. We first started to see signs of this during very late December last year and since then the market has continued to improve. It is now increasingly possible to secure discounts at renewal as well as improvements to policy wordings. There have been many cases where we have seen reductions, and in particular scenarios discounts of 30% plus have been achieved.

Many underwriters began 2010 believing that given the recent influx of claims, they would be able to continue to secure increases on their renewal books for at least the first half of the year and thereafter perhaps see the first signs of the market flattening out. The reality has been somewhat different, with a number of new entrants to the market needing to secure premium income more quickly than anticipated and hence bringing about what many underwriters will see as a premature end to the hard market.

That said it is still very much a tale of two markets with the old guard of established players still looking to resist discounts and new markets needing to be aggressive to gain market share. This ‘transitional’ market will not last forever and at some point there will be an acceptance across the entire market that there is downward movement in rates, hence insurers will be far more likely to offer discounts at renewal at the outset of negotiations, indeed we are starting to see signs of this already.

So, how to best take advantage of the current market? Buyers of smaller limits of indemnity, (up to GBP 50 million) with their increased buying power will be best placed to take advantage of these conditions. Currently, most underwriters are not volunteering discounts so more than ever the ability of your broker to leverage the market and generate effective competition are vitally important. Additionally commencing the renewal process early, ensuring plenty of time to deliver and consider options will always reap benefits.
CRIME INSURANCE FOR FINANCIAL INSTITUTIONS

The Crime Policy has been criticised in the past for the area of exposure which it leaves uncovered in terms of fraud, which does not involve the specified instruments and specified means of fraud (for example, forgery, fraudulent alteration, counterfeiting or presentation of lost or stolen securities are covered, but misrepresentation of facts in documentary form or wholly fictitious instruments are left uncovered). While it is true that there is a gap in this way, insurers have always felt that they cannot offer an open-ended insurance for fraud without it being demonstrable that checks and tests designed to prevent fraud have been overcome. In terms of documentary fraud, this involves the specified types of securities or negotiable instruments or in terms of the electronic communications cover, ‘testing’ of communications (in telephonic communications, for example) might be required as a pre-requisite for cover.

Fraud which is perpetrated by means of false pretences or identity theft remains uninsured so long as no actual forgery, fraudulent alteration or counterfeiting is used. While the policy covers theft of (financial) property by false pretences by persons on the Insured’s premises, it does not do so elsewhere other than the ‘physical loss’ (premises and transit) insuring clauses.

In contrast, the Employee Dishonesty cover is virtually all risks (any dishonesty or fraudulent by an employee, subject only to the intent provisions described later). The Computer and Electronic Crime cover too, could at least be described as ‘comprehensive’ covering as it does, loss resulting from any fraudulent input or modification of data or programmes. The limitations to electronic fraud are fewer than those in documentary fraud and tend to appear as limitations of the systems (perhaps the Assured’s computer only or named transfer systems in some of the more restrictive policies).

Generally speaking, the computer and electronic fraud cover is undoubtedly wider than that provided for documentary fraud. This is due to a perception among insurers that there have been few successful computer crimes compared to the volume of documentary fraud. However, there are some signs that this attitude is changing and we may see more restrictions placed on the cover, which will seek to exclude ‘pure misrepresentation’ in a parallel fashion to the exclusion of this exposure in the documentary cover.

However, to take a current example, where identity theft or ‘phishing’ is concerned, computer and electronic fraud cover responds and covers purely on the basis that the input of data eventually used by the thieves or ‘phishers’ is fraudulent – while the documentary fraud cover would only respond to such a loss (where perhaps false identity papers were used, for example) if there were also fraudulent alteration or forgery in specified documents (cheques, instructions, securities etc.).

Unfortunately, there seems to be no early prospect of Insurers wishing to extend the Crime Policy in the current market conditions and purchasers need to have their eyes open to the fact that the Crime Policy is not a complete solution. It is a vital element in an overall approach to risk management but experience shows that a thorough review and reconstruction of policies is essential to ensure maximum cover is obtained.

The Crime Policy therefore provides a significant role in transferring the crime risk but should be regarded as part of an overall risk management strategy – one which needs to be used in a discriminating way to ‘dove-tail’ with risk mapping, profiling and other risk management tools within the organisation.

WHAT DOES IT COVER?

Direct financial loss which the institution has sustained at any time but discovers during the policy period resulting from:

Employee Dishonesty

Dishonest or fraudulent acts of employees or those in collusion with them, provided that if the loss involves trading and loans activities, the acts:

(i) were intended to and result in improper financial gain (other than ‘normal employee remuneration’) for the employee OR
(ii) result in unauthorised transfers to innocent third parties which the institution cannot legally recover.

The Crime Policy does not include cover for unauthorised trading unless improper financial gain for the employee was intended.

Physical (financial) Property

All physical risks to financial instruments (securities, negotiables, other) in transit or on premises.

The value of subscription rights from loss of securities or other instruments is included.

Damage to offices and contents caused by break in or safe burglary is included – excluding computer equipment and fire risks.

Documentary Fraud

1. Forgery or fraudulent alteration of:
   - cheques and other negotiable instruments.
   - written or printed transfer instructions.
   - life office documentation (policy loan agreements, death certificates and similar).
   - mortgage documentation (limited to signatures obtained on mortgages, real property deeds of trust or like instruments pertaining to heritable property or assignments of such through false pretences or deception (it would not extend to include ‘ringing’ or falsely inflated values in the mortgage application or applications by fictitious applicants).
2. Reliance on forged, fraudulently altered, counterfeit, lost or stolen Securities.

'Securities' typically includes a wide definition, including all types of stock, shares and scrip, certificates, bonds etc., stock transfers, assignments, partnership guarantees and documents involved in dematerialised securities.

3. The institution having guaranteed or witnessed signatures on securities where the signature is forged or there is a fraudulent alteration or the instrument is lost or stolen.

4. The institution having been deceived as to the identity of any person for the purposes of buying or selling (financial) property.

**Counterfeit currency**

The institution’s receipt of any counterfeit currency purporting to be legal tender.

**Legal Fees**

The Crime Policy covers loss of funds and (financial) property in the institution’s custody as if it were first party loss to the institution, regardless of ultimate ownership. If customers or clients of the institution assert that they have sustained a loss, the bond covers legal defence costs if the loss claimed (if it is proved) would constitute a loss covered by the bond.

**Electronic Communications and Computer Fraud**

Loss through fraudulently corrupted or fraudulently input data or programmes – either on computers or inward electronic communications (including telephonic voice instructions) for funds transfers, costs of reconstituting and verifying data and programmes following such fraudulent acts or following malicious attacks (including virus and other malicious code).

The institution’s liability for reliance of customers or financial institutions on data in its computer or electronic communications which fraudulently purport to have been sent by the institution.

Extension can be obtained for:

- Liability for failure to carry out stop cheque instructions or failure to honour valid cheques.
- Theft of funds inadvertently transferred to the wrong account or in the wrong amount by or on behalf of the institution and where legal recovery fails.
- Theft of funds transferred by the institution under the terms of the Settlement Bank Agreement between Euroclear and the institution.

Extortion demands – covering the amount of ransom paid following threats to the institution’s personnel, relations or invitees or threats to the institution’s property or computer systems.

**WHAT DOES IT NOT COVER/ TYPICAL EXCLUSIONS**

Documentary Fraud other than in respect of the named instruments and forgery, fraudulent alteration or counterfeit of such (as detailed above in 'Documentary Fraud'). This would exclude cover for misrepresentation in loan applications etc., or false pretences/identity theft involving paper documents unless forged signatures or fraudulent alteration were involved.

Identity theft, which makes use of PIN or other security codes to access computer systems is not, however, excluded if it involves the fraudulent input of data.

Dishonest or fraudulent acts of directors unless performing employee activities.

Loss through loan defaults unless caused by Employee Dishonesty or Documentary Fraud.

Factoring/invoice discounting/accounts receivable, forgery or fraudulent alteration of bills of lading, trust receipts and similar.

Payments from customer accounts against items not finally cleared, including cheque kiting and ‘cross-firing’.

Safe Deposit Boxes (policy can be extended to cover).

Wear, tear, gradual deterioration, moth, vermin.

Travellers’ Cheques (other than Employee Dishonesty losses).

Loss involving plastic cards.

Loss resulting purely from trading.

Loss of trade secret or other confidential information (not applicable to loss resulting from computer fraud making use of such information).

Loss caused by any employee’s further acts or omissions after the institution has discovered that the employee has committed a dishonest or fraudulent act.

Loss not first discovered in the policy period (awareness of likely circumstances would constitute ‘first discovery’).

(Financial) property in the post – the policy can be extended to cover ‘cash letters’ (deliveries of non-negotiables/cleared cheques etc.) or mailings via registered or recorded delivery but a sub-limit might be applied to each mailing.

Applicable to computer and electronic communications fraud: Loss resulting from input by persons authorised to use a customer’s authentication mechanism unless exceeding the authorised level for a fraudulent purpose.
HOW DO WORDINGS DIFFER FOR THIS CLASS?

Policies do not differ a great deal in ‘headline’ terms but ‘nuances’ arise through poor drafting in insurers’ offered policies and brokers seek to get absolute clarity on many points as well as to widen cover. The breadth of cover delivered by the text depends, as one would expect, on size of the institution and premium paid, but also, significantly, on the ability of the broker to perform a thorough review and upgrade exercise. The covers indicated above are typical of cover for most organisations.

More ‘narrow’ policies might apply (for example only):

– The ‘intent’ for gain provisions in the Employee Dishonesty cover to all losses (not simply trading and loans)
– Restrictions as to premises – the institution’s own or recognised places of safe deposit or, as to transits – by employee/messenger/armoured motor vehicle or security carrier
– ‘Tighter’ conditions as to ‘discovery of loss’ (usually it is possible to restrict policy conditions which address the institution’s duty to notify discovery of loss, by providing that the duty is that of named departments only – risk management or other. This minimises or avoids the dangers of policy penalties such as avoidance of the claim by insurers for ‘late notice’ which results from unreported awareness of loss at a junior level in the institution)
– A narrower definition of ‘Securities’ and absence of cover for life office documentation fraud or mortgage documentation fraud
– Absence of the extensions for:
  – Liability for failure to stop cheques or honour valid cheques
  – Theft of funds inadvertently transferred to the wrong party
  – Theft of funds transferred under the terms of the Settlement Bank Agreement between Euroclear and the institution
  – Extortion demands
– A more rigorous approach to proposal disclosures (at the optimum, insurers will not void the policy for innocent misrepresentation or failure to disclose matters in the proposal)
– Less favourable conditions as to automatic cover for acquired subsidiaries (a reasonable standard of cover for this would be 90 days automatic cover and notification to insurers only required where the asset size exceeds, say, 15% of the institution’s gross assets.)
– A more restrictive approach to computer and electronic communications fraud cover by means of limiting cover to corruption of data on the Assured’s own systems and by adopting a ‘named systems’ approach to electronic communications – SWIFT, BACS etc.
– A retroactive date (when first accepting the risk an Insurer may exclude loss sustained prior to the inception of the policy – at best, there should be no restriction of when loss is sustained – whether before or during the policy period, provided it is ‘first discovered’ (see above) during the policy period)

TYPICAL LENGTH OF A POLICY

12 months

Notable Claims

Diversion of funds by employees from infrequently used or dormant accounts, acceptance of inducements by customers to the employee to arrange loans which breach the institution’s internal guidelines and controls, or other collusion with outside third parties, or the arrangement of entirely fictitious loans by employees.

Hold ups, robbery, extortion by holding families of staff to ransom, forcing the staff member to use his knowledge of security codes to remove funds from safes etc.

Theft involving forged cheques, forged, counterfeit or lost or stolen securities.

‘Keylogging’, bogus transfer instructions making use of stolen security codes and other attempts to transfer funds out of accounts by computer hackers.

Theft of funds inadvertently transferred to the incorrect recipient or transferred for the wrong amount (overpayment) to the correct recipient.

Trevor Simpson
Wording Specialist
Willis Limited

To discuss your insurance arrangements with the Willis FI team please call your Account Executive or Paul Richards on +44 (0)20 7558 9240.