Autumn 2014

haysmacintyre
chartered accountants & tax advisers

# PIMBs BRIEFING

No 1 "Overall Service Award" 2011, 2012 & 2013 | "Charity Expertise Award" 2011, 2012 & 2013 | *Charity Finance* Audit Survey

Letter from the Editor | Subscription Apportionments - Are They At Risk | How Robust Are Your Internal Financial Controls? | Increasing Importance of Data Protection

# LETTER FROM THE EDITORS

**Welcome to the Autumn edition of our briefing for professional institutes and membership bodies.**

In this edition Phil Salmon, haysmacintyre VAT Partner, looks at the apportionment of subscriptions for VAT purposes and Simon Bulleyment, Director of haysmacintyre IT Consultants Limited, covers the importance of data protection.

In the last issue of our briefing, Mark Leckie gave information and tips to help you make sure that your organisation doesn't fall victim to internet banking fraud. But what about other types of fraud? In this edition we consider the robustness of internal controls.

In October we hosted, for the third year, the launch of the PARN Financial Benchmarking Survey which aims to provide the professional body sector with analysis of key financial information from annual reports in order to compare individual organisations' performance.

This year's report also compiled the results of a survey on reserves: the level of reserves held, the reasons for holding reserves and the process of reviewing the reserves policy. One of the key messages from the survey is that, while there are a number of areas where the sector is adopting best practice and common principles, there is not a standard approach to reserves policies. So is it time for you to review your reserves policy?

We will be tackling this topic at a PARN Finance Special Interest Group in the New Year as well as providing updates on VAT and best practice in financial reporting.

Further information on the Financial Benchmarking Survey can be found at http://www.parnglobal.com.

If you have any feedback on this edition of the briefing, or wish to discuss any of the matters raised, do contact one of our team

**Jeremy Beard,** Partner and Head of PIMBs
**T** 020 7969 5503 **E** jbeard@haysmacintyre.com

**Kathryn Burton,** Partner
**T** 020 7969 5515 **E** kburton@haysmacintyre.com

# SUBSCRIPTION APPORTIONMENTS - ARE THEY AT RISK?

Many membership bodies apportion their subscriptions for VAT purposes to reflect the underlying benefits provided to members. For example if the starting point is that your subscription would be standard-rated, but you provide members with a hard copy journal, then the apportionment allows you to treat part of your subscription as zero-rated and account for less output tax.

Similarly, if the starting point is that the subscription would be exempt, then such an apportionment would allow you to recover more input tax.

Such apportionments have been allowed since one of the very first VAT cases, the Automobile Association back in 1974. More recently, as case law has developed, HMRC has allowed their continued use by concession.

A recent case has cast doubt on whether such apportionments continue to work for VAT. The case was that of the Serpentine Trust Ltd and the membership scheme concerned was a "Friends'" scheme common amongst arts charities.

In common with most such schemes, the basic premise is that people sign up to give regular amounts, usually at different tiers. In return for their gift or donation they receive certain benefits. The benefits almost invariably cost much less than the amount donated and vary according to the amount donated. The idea is that part of the amount given is regarded as a donation, and part as payments for the benefits received.

The problem with this type of supporter scheme is that in the 1994 Court of Session case of Tron Theatre. In that case supporters donated money to fund the refurbishment of the theatre and donors were acknowledged by way of a plaque bearing their name on the back of a seat in the refurbished theatre. The Court of Session held that the donations were actually consideration for a supply of the plaques and therefore VAT inclusive, even though the value of the plaque bore no relation to the amount donated and the fact that the plaques remained in the theatre such that there was no transfer of ownership.

Since that time, HMRC has tended to accept the concept of a split donation/consideration but this case throws open the question of whether they will continue to do so.

There were five different supporter schemes (tiers), but the case concerned only four of them. In the other one, HMRC had agreed that a certain amount was payment for the benefits and the balance was a donation. The problem with the other four is that they appear to have treated all of the money as a donation. HMRC took issue with this and assessed accordingly.

At the hearing the Trust advanced three arguments why it was correct not to have accounted for VAT. Firstly, it argued that the benefits were de minimis and not provided in return for the payments made.

This was essentially the question that had been looked at in Tron and whether there had to be some proportionality between the value of the benefit and the amount of the payment. The Tribunal expressed some doubts as to whether the value of the benefits were as low as the Trust argued, but in any event said that this was irrelevant. It came to the view that objectively the benefits were for the consideration, and that they had value to the supporters even if the cost was below that value.

The second argument was that the amount paid should be apportioned, as was the case with the fifth category/tier of the scheme which was not being challenged.

Importantly, this was also the case for the other tiers of membership for subsequent periods, but not for the periods which were the subject of the assessment. This also drew on Tron, and the Tribunal held that once it had been decided that the payment was for the benefits, then even if the supply was grossly overvalued it made no difference, the amount paid was consideration as that was what had been agreed between the parties.

However, the Tribunal did go on to say that if the Trust had offered benefits for a fixed price and specified anything additional was a donation, then the element of donation would not be paid for the benefits.

The last argument was that if there could be no apportionment between the donation and the consideration, then there should be an apportionment anyway to reflect the fact that some of the benefits were zero-rated, and some were exempt.

The Tribunal decided that there was a single supply of the opportunity to partake of exclusive events at, and offers by, the Gallery.

The Tribunal specifically did not consider the extra statutory concession allowing such apportionments because the parties both accepted that the Tribunal did not have the jurisdiction to determine the application of a concession, though it did say that HMRC's view that the concession only applied to membership bodies, where members have a say in the governance of the organisation, unlike this type of membership scheme.

So where does the case leave us? It would not be correct to say that subscription apportionments can no longer be made. For membership bodies where the body is governed by its members the extra statutory concession is still clearly available. The only threat to that appears to be whether HMRC decide to withdraw the concession. If they do then the decision seems to suggest that an apportionment of benefits between standard-rated, zero-rated and exempt elements may not be possible, but it should still be possible to have a split donation/consideration type scheme.

For friends type schemes it seems as though HMRC are lining up to argue that the concession does not apply to them even if it remains, but again a donation/consideration would continue to work. Whether HMRC would succeed with such an argument, where their guidance clearly does indicate that the consideration can itself be split into elements which are zero-rated, is the question that the case does not address, and it seems to be likely that this would only be settled on a judicial review, or by taking a case through to the Upper Tribunal.

For now, you should review your schemes to ensure it is apparent to supporters that they can avail themselves of the benefits by payment of the minimum amount, but otherwise continue as you have been doing. But, be aware that this is an area which now seems to be on HMRC's radar and the days of the apportionment may be limited.

**Phil Salmon,** VAT partner
**T** 020 7969 5611 **E** psalmon@haysmacintyre.com

# HOW ROBUST ARE YOUR INTERNAL FINANCIAL CONTROLS?

Council members have a legal duty to safeguard the assets of their organisation, so that they can be applied for its intended purposes. It can be difficult for Council members, who are often not involved in the day to day running of the organisation, to know what types of financial controls should be in place.

The good news is there is a lot of useful guidance available to help. The first step is: don't assume that it won't happen to you. The Annual Fraud Indicator, issued by the National Fraud Authority in 2013, highlighted that:

- Participants from the private sector estimated that, on average, fraud losses as a proportion of turnover could be in the region of 0.54 per cent, with 0.18 per cent lost to detected fraud and 0.36 per cent lost to hidden or undetected fraud. This is approximately equivalent to £15.9 billion per annum.
- Fraud against the public sector is estimated to be £20.6 billion per annum. The estimate of possible public sector fraud losses includes losses to local and central government, as well as to the tax system.
- Fraud against the charity sector is estimated to have cost registered charities £147.3m in 2011/12. Of the charities that responded to this survey, almost one in ten had experienced fraud, most commonly payment or banking fraud.
- Fraud against individuals in the UK equates to a loss of £9.1 billion per annum, based on estimates of the scale of mass-marketing fraud, identity fraud, online ticket fraud, private rental property fraud and electricity prepayment meter scams.

So where can you look for guidance on how robust your internal controls are?

A good place to start is the Charity Commission's guidance on fraud, Safeguarding your Charity: Compliance Toolkit, which is available on their website (search on the Charity Commission site for 'Compliance Toolkit') and gives practical guidance on what Trustees should be doing to mitigate the risk of fraud in their charity. It also outlines ten tips for Trustees which are relevant for all not for profit organisations, not just charities:

- Review financial controls regularly and keep them up to date
- Segregate duties in the finance department
- Reconcile financial records to supporting documentation such as receipts and invoices
- Don't take short cuts such as presigning cheques, or sharing bank passwords
- Keep an up to date fixed asset register
- Ensure that online banking arrangements are secure and require two authorisers
- Take up references when recruiting staff
- Carry out due diligence on grant applicants
- Ensure that Trustees receive regular, appropriate financial information
- Make sure you know what to do and who to inform if you suspect fraud

The Charity Commission's checklist of internal controls (CC8) is also a useful tool for assessing your existing procedures – search for 'Internal Controls Checklist' on their website.

**If you would like more information on how to strengthen your internal controls, we would be happy to support you.**

**Tom Brain,** Senior Charities and Not for Profit Manager
**T** 020 7969 5670 **E** tbrain@haysmacintyre.com

# INCREASING IMPORTANCE OF DATA PROTECTION

Since 1 March 2000 many organisations have had to become compliant with the Data Protection Act 1998 (DPA). This places a series of legal obligations on those who handle personal data about individuals, this being information which relates to an identifiable living individual and that is processed as data. Examples might include customer or member details held in CRM systems, such as name, address, date of birth and telephone number details.

Within the DPA are eight data protection principles which define how data should be used and protected. Amongst those stating that data must be processed fairly, for specific purposes and must be relevant, is principle seven which states that:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, damage to, personal data."

In a nutshell, what this is really saying is that for organisations which store personal data on their IT system, there needs to be adequate security controls in place so that data cannot be deliberately or accidentally compromised. More specifically, the DPA states that security controls should be appropriate to:

- the nature of the information in question; and
- the harm that might result from its improper use, or from its accidental loss or destruction.

Before an organisation implements any form of security controls, the first step is to perform an information risk assessment to review which personal data is being held, how it is used, how valuable, sensitive and confidential it is and what damage or distress could be caused to individuals if there was a security breach. As part of the risk assessment, organisations must also consider if they are using third-parties which hold or use personal data on their behalf.

The DPA does not and cannot define which security measures should be implemented, but the following is a list of areas which would usually be considered:

- Security Policies – is there a policy in place, who manages and updates it, have staff been made aware of it?

- Personal Security – are staff/contractors aware of their security responsibilities, and how to recognise and report security incidents, suspected weaknesses or threats to the system?
- Physical & Environmental Security – what security controls are in place to protect physical access to the IT system and data. Without appropriate technical and/or procedural controls, it might be possible for an unauthorised individual to plug a laptop into a spare network connection in a visitor area and gain access to personal details stored on it, without requiring any type of network username and password. Or worse still, plug a laptop into it and launch a malicious application which starts deleting data!
- Organisational & Operational Management – who within the organisation is responsible for security, how are data backups performed and more importantly are backups tested on a regular basis to ensure that data can actually be restored in the event that loss occurs? Often the weakest link within an organisation's security controls are the end-users themselves. Hackers will often exploit people in an attempt to get them to do something they shouldn't which can result in data compromise e.g. a hacker pretending to be from an IT department who phones a user and asks them to reveal their password! These type of attacks are much simpler and are often more effective for a hacker than attempting to exploit vulnerabilities in technical controls, such as firewalls. Organisations must therefore ensure they have considered the risk from social engineering and have educated end-users so they do not fall victim to such attacks.
- Virus Protection & Endpoint Security – what controls are in place to prevent viruses, spyware and other malicious software from infecting PCs and laptops?
- Internet Security – what technical controls are in place to protect the internal network and server resources from Internet launched attacks?
- Remote and Wireless Access Security – remote access technologies, such as the use of VPNs, and WiFi technology is commonplace within most organisations but how are these systems controlled to ensure they are accessible only by authorised users?
- Security of Laptops, Tablets & Smartphones – organisations will often allow laptops to download files to them and the likes of iPhones, iPads and Android devices to access internal data, such as email which might have attachments containing personal data. Controls need to be considered to ensure that data is secure should the devices become lost or stolen.
- Third party contracts – where third parties are storing or processing data on your behalf, are their security procedures robust and their responsibilities clearly set out in a contract?

The Information Commissioner's Office (ICO) is the UK's independent authority which has overall responsibility for data protection and it essentially does three things:

- Promotes good practice in handling personal data, and gives advice and guidance on data protection.
- Keeps a register of organisations that are required to notify the ICO about their information-processing activities.
- Takes action to enforce compliance with the DPA and brings prosecutions for offences committed under it.

Over the last few years the ICO has demonstrated that it is not afraid to make examples out of organisations which fail to protect personal details. Recent cases include:

- The Ministry of Justice was fined £180,000 for failing to protect sensitive and confidential data relating to 3,000 prisoners stored on an unencrypted hard drive which later became lost (this followed a similar incident which had occurred several years earlier).
- The British Pregnancy Advice Service (BPAS) was fined £200,000 for failing to protect the personal data of thousands of people held on their website. The ICO discovered that people had been leaving their details (name, address, telephone number) to request a call back. BPAS were unaware this data was being stored, therefore failed to encrypt it and a hacker exploited a vulnerability in the website and gained access to the information.

There is little doubt there will be many other examples in the future of the ICO handing out large fines to organisations who fall foul of the DPA. As well as the financial loss incurred with fines, there is also the reputational risk to consider. If the ICO was to make an example of an organisation which mishandled the personal data of donors, it's a safe bet that some would consider finding a new organisation to support which took better care of their details.

**If you require further information or advice on the implications of the DPA or other IT security more generally, haysmacintyre IT Consultants Limited, are able to assist.**

**Simon Bulleyment**, Director of haysmacintrye IT Consultants Limited
**T** 020 7969 5675 **E** sbulleyment@haysmacintyre.com

haysmacintyre
chartered accountants & tax advisers

# Future events

| | |
|---|---|
| PARN Special Interest Group* | 9 February 2015 |
| haysmacintyre VAT Exchange | 25 March 2015 |
| Training courses for charity trustees 2014/2015 | Multiple dates available on our website |
| Network of Women Chairs | Multiple dates available on our website |

*Open to members of PARN only

For further information on these events please visit www.haysmacintyre.com/events

Should you wish to receive an electronic version of our briefing in the future please email Charlotte Gibbons on cgibbons@haysmacintyre.com





haysmacintyre
26 Red Lion Square
London
WC1R 4AG

**T** 020 7969 5500 **F** 020 7969 5600
**E** marketing@haysmacintyre.com
www.haysmacintyre.com
@haysmacintyre