Electronic reliability

Data feeds have become a critical component of SMSF administration in recent years. Ron Phipps-Ellis gives an insight on the implications of this development for practitioners and particularly auditors.

RON PHIPPS-ELLIS is executive director of Evolv.

Data feeds have radically changed the traditional approach to accounting. The days of manually entering transactions via a debit and credit journal entry are almost history. Now it's all about matching transactions that have not been automatically allocated.

It is important to understand the process of how this data is accessed.

Surprisingly, requesting access to electronic data is still a manual paper-based process. Software providers either access data direct from the source or via a data aggregator, which acts as an intermediary. All parties must first obtain the customer's written authority and forward this onto the source providers that hold the data. There are two authority forms that need to be completed.

Individuals give authority to their broker or adviser via a third-party authority form. The adviser then sends this request to the institution to grant the requestor authority to download their clients' data. This authority may cover a single product or multiple products from that institution.

Alternatively, an account holder authority form is given at client level. The client sends the request to the institution to grant the software provider or data aggregator authority to download for specific accounts.

It seems logical the ownership of the data remains with the customer who has requested it and ultimately pays for it at some point in the service process.

There are a number of ways to receive data electronically.

Direct data feed: A direct data feed, which is received from the source provider, is currently the

Continued on next page ▶

Table: Receiving data electronically: advantages and disadvantages

	Advantages	Disadvantages
Direct data feed	Higher-quality data	Higher cost
	Quality resolution process	Authority forms
	Efficient	Not always retrospective
Screen scraping	Easier to implement	Less quality data
	Lower cost	Customer log-in details required
		No data resolution process
Optical character recognition	Alternative when direct feed not available	Less quality data
	No customer authorisation required	

▸ ***Continued from previous page***

preferred option. Currently, this is restricted to accessing cash transactions from financial institutions. The process of accessing share transactions is sourced via authorised brokers and not from the share registries. Managed fund and wrap providers can produce their periodic reports electronically.

Most banks, building societies and fund managers release their feeds daily. For bank transactions it is normally at 6am, or 11.30am for SMSFs. The majority of credit unions only release feeds monthly.

However, not all feed sources can provide historical data. In these situations the feed only commences from the time it is activated. This often means there is a combination of direct data feeds and manually inputted transactions in a data file.

Screen scraping:
This involves accessing customers' data via a user interface, usually by internet banking or a share registry, and then running a process to expose data from a screen or a script to obtain a transaction listing.

There are a number of screen-scraping providers that offer this service at a wholesale level. But privacy and reliability are still major issues. It is still common practice to verify listed securities transactions manually by logging into share registries and inputting a customer's holder identification number/security reference number and postcode. Interestingly, this often occurs without the express consent of the customer.

Optical character recognition (OCR)::
OCR of a source document is where a PDF is downloaded and key information is electronically extracted into another format.

Data security

Be aware that, as a service provider, you are responsible for the safe electronic storage and any transmission of your customers' data.

The *Privacy Amendment Act 2012* came into effect on 12 March 2014.

This act deals with the security of personal information and requires organisations (individuals, bodies corporate and partnerships) to abide by rules in managing personal information.

You should implement a formal cybersecurity plan that addresses:

1. Risk assessment,
2. Policies to mitigate risk,
3. A framework for identification of breaches and reporting thresholds, and
4. Ensuring a proper cyber-incident response plan is rehearsed and tested.

You should also consider a cyber insurance policy.

Once the data has been received by your software provider, it is now up to the user to determine how reliable these data-fed transactions really are.

So the quality of data becomes the most paramount issue for any user of data-fed transactions.

A common term used by data aggregators for direct data feeds is 'accounting-grade data'.

Obviously this means data can be relied on without the need to verify back to paper-based statements issued from the source.

The two main determinants of reliability are:

Discrepancies in data feeds must be manually corrected by the data aggregators, the software providers that access these feeds or by the end users. This detracts from the acclaimed time savings that automation should provide.

1. Completeness – transactions for a given period must have all been received and must be free of omissions. Accounts incorrectly removed or closed is one measure criteria.
2. Accuracy – transactions must be correct and reconcile back to a balance. Opening and closing balances not tallying is the main measure criteria. (Opening balance + transactions = closing balance is an obvious script that is run over bank data feeds. But confirming a closing holdings balance for listed securities is not so simple).

According to SISS Data director Grant Augustin, some common errors of direct data feeds that are received from financial institutions are:

- account number and BSB changes,
- transactions do not reconcile back to closing balance,
- data has not been received for an account,
- incorrect signage of debits and credits, and
- false duplicated transactions (two identical transactions).

The extent of the occurrence of these types of discrepancies is difficult to quantify.

It is interesting to note there doesn't appear to be any minimum industry mechanism ensuring the consistent quality of data feeds that are released from financial institutions.

The result is that discrepancies in data feeds must be manually corrected by the data aggregators, the software providers that access these feeds or by the end users. This detracts from the acclaimed time savings that automation should provide.

Some questions to consider when using software that relies on data feeds:

- How does it source the data feeds?
- How formal is the process to manage, track and report on data quality?
- What are the processes to ensure completeness and accuracy of data?
- What are the rectification processes when an error or omission is detected?
- Is future data processing halted until rectification is completed?
- How often is data reconciled?
- How often are results on data quality reported?
- What are the data error tolerance levels?

Some guidance on the extent of reliance on data feeds is given in auditing standard ASAE 3402, which commenced on 1 January 2015 and applies to assurance engagements on controls at a service organisation.

This is an important report some of the super software suppliers are now providing on the reliability of data-fed transactions.

The extent of a user's reliance on this report and hence the underlying data feeds depends on its scope.

Ideally the report of the service organisation should be a type two report and should include:

1. Description of its system and if it is fairly presented as it was designed and implemented throughout the period,
2. The controls were suitably designed throughout the specified period, and
3. The controls operated effectively.

A careful analysis of this report is required by any user (including administrators, advisers, accountants and especially auditors) to determine how much reliance a user can place on data-fed transactions.

There are many exceptions reports generated from the super audit software providers that detail errors in data feeds and any manual manipulation that has occurred for each data-fed transaction. These errors are resolved usually periodically throughout the year by the super fund accountants/ administrators as part of the accounts preparation process.

Auditors, however, have to go looking for these exceptions reports inside the software programs and perform their own analysis of each report to determine the extent to which they can be relied on. This requires some IT capability, but considerable analysis and judgment given the inherent risk of litigation for undetected errors.

So the controversial questions here are:

1. What level of reliance can auditors place on ASEA 3402 reports on the software programs?
2. To what extent can auditors rely on the data-fed exceptions reports inside the software programs without doing any testing procedures?
3. Can algorithms that underlie data analytics procedures to automatically perform risk analysis on funds fully replace traditional audit procedures and human judgment?

There will be many approaches adopted by auditors depending on their risk appetites. In my opinion there is still a requirement to perform at least a base level of alternative substantive testing procedures on certain data-fed transactions in order to obtain sufficient appropriate audit evidence in complying with the audit standards, and to appropriately report on the 22 sections and Superannuation Industry (Supervision) (SIS) Regulations in the audit report.

Documentation is fundamental to the audit file. It is important auditors continue to thoroughly document their audit approach, particularly to data-fed transaction testing to be able to justify how they have satisfied each audit assertion and relevant SIS provision.

So, I'm not expecting an SMSF audit can be fully automated anytime soon. The issue of quality data feeds from source providers might take some time to resolve. Moreover, it will be many years before the level of human judgment required in an audit can be substituted by data feeds, exception-based auditing and algorithms alone. ▼