Abstract

Research in the USA shows an increase in branches and in the number of customers who make regular use of branch facilities. Alternative delivery "channels" must be integrated into co-ordinated customer-centered policies. Customer information is central to developing and maintaining these policies. Recent regulatory developments will have an impact on planning the management of customer information.

1. Delivery "channels"

E-commerce offers banks the opportunity to provide cheaper methods of delivering services. Research conducted by the Gartner Group in the USA shows that a transaction conducted through a teller costs between $1 and $2. A transaction conducted via PC/Internet is between $0.02 and $0.10. The precision of these figures may be doubted or may be inapplicable to other countries, but the relative costs of the two forms is probably the same everywhere.

E-commerce is not new for Australian banks. ATMs have provided an alternative to branch/teller based transactions for some years. Although ATM transactions are much cheaper than teller assisted transactions, there is another, perhaps more important, effect: generous ATM support is an important factor in maintaining customer loyalty for non-ATM based transactions.

Both branch and ATM positioning is based on physical location. Newer delivery channels are based on more abstract considerations. The development of telephone banking and, even more importantly, PC/Internet banking is based on design and marketing factors that might be called "channel location".

The development of alternative delivery channels is far from complete. Access to banking services through personal digital assistants, interactive TV, and various wireless technologies will be developed and matured.

2. Coexistence

The salient characteristic of these alternative delivery channels is that they do not replace branch services. It is not necessary to rely upon press reports or anecdotal evidence for this: research in the USA shows that there has been a growth in the number of branches during the 1990s. Further, this grown has accelerated since 1996 with the number of branches growing by 1 to 1.5% per year.

This has been accompanied by a growth in the number of customers who use branch services on a regular basis. This is in spite of bank predictions of a decline and, in many cases, the implementation of punitive policies intended to force such a decline.

This is not to say that branch structure must remain the same. Different ownership structures are being explored both in the USA and in Australia. The range of facilities that branches offer might become more specialised rather than being universally full-feature.

In might be argued that these findings are not relevant to Australia because of the dramatically different banking and social structure of the two countries. This might indeed be the case, but it would be dangerous to conclude that without some serious research to establish just what the differences are. Making the wrong decision here leaves the field open to competitors who are exploiting the weakness of banks.

The American research and common sense suggest that the alternative delivery channels must coexist with and compliment the branch structure of banks. Indeed, it is the competitive advantage enjoyed by banks over new entrant competitors. While e-commerce delivery channels offer cheap entry for new competitors, the intelligent integration of alternative delivery channels with the traditional branch access can work to the banks' advantage in gaining and retaining the customer base.

3. Customer information management

E-commerce merely provides the alternative delivery channels. The difficult business decisions are to determine what to deliver, whom to target and how to ensure that the relationship with customers is maintained and enhanced.

A sophisticated approach to these problems requires a high-level customer information management system (CIMS). The most general and useful form of CIMS is the so-called "data warehouse" coupled with applications software. The data warehouse is characterised by:

- wide view of purpose;
- retention of historical data;
- analytical viewpoint (as opposed to operational); and
- integrated end-user functions.

The data warehouse usually incorporates all enterprise customer information. The integrated end-user functions permit the warehouse to be used for functions (eg, billing) that were previously achieved by smaller or individual databases.

From the viewpoint of developing e-commerce solutions, the importance of the data warehouse is its use as an analytical tool. It may be used:

- to discover or explore customer segmentation;
- for predictive modeling;
- profitability analysis; and
- exploring the development of complex event-based triggers and other marketing tools.

Developing an integrated functional data warehouse is no small task.

4. Regulatory developments - Privacy

There are several regulatory developments which must be addressed if expensive mistakes are to be avoided. The most important of these is the new Privacy Amendment (Private Sector) Bill 2000.

The Privacy Amendment (Private Sector) Bill 200 was introduced in Parliament on 12 April. If enacted, the legislation will require most "organisations" to adhere to standards when handling "personal information". The National Privacy Principles (NPPs) will be the minimum standard. These principles regulate the collection, use and disclosure, rights of access and correction, and storage of personal information. Special requirements apply to "sensitive information" and "health information".

4.1 Data covered

The NPPs regulate the handling of "Personal information". The phrase is defined in the Privacy Act as

"information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

Special rules apply to "sensitive information". The Bill lists certain types of information or opinions about an individual which are thought to be "sensitive". The list includes such matters as race and various beliefs, activities, memberships, sexual behaviour and criminal records. Financial information about a person is not "sensitive information".

Not all of the NPPs apply to "old" data, that is, data collected before you are required to comply with the Act.[1]

This "old data" exemption is not as generous as it seems. You may use the data for any purpose, but before use you must take reasonable steps to ensure that it is accurate, complete and up-to-date[2]

Most "old data" will require regular updating. The Attorney-General has indicated that when "old data" is updated, it is no longer old and so is subject to all of the NPPs.[3]

If you intend to make use of the "old data" exceptions, you must implement systems which will clearly segregate "old data". You must ensure that when data is updated that it is no longer classified as "old".

Many organisations will find that this trouble and expense is unjustified for the limited exclusions granted.

4.2 Use and disclosure

The basic rule is that personal information may only be used for the "primary purpose" for which it was collected. There are rules for the use of the information for any "secondary purpose".

For retail bankers, the most important exceptions are those for direct marketing and the "consent" rule.

4.3 Direct marketing

Direct marketing is one of the most important uses for a CIM system. This is particularly so if "trigger events" are used to initiate a contact with a customer.

Non-sensitive personal information may be used or disclosed for direct marketing purposes. This is so even if the individual has not consented and would not normally expect that the information would be so used. However, some conditions apply:

- it must be impracticable to seek the individual's consent before the use; and
- there must be no charge to the individual for honouring a request not to receive direct marketing communications; and

---

[1]Section 16B.

[2]See NPP3.

[3]See the Explanatory Memorandum.

- the individual has not made a request not to receive direct marketing communications; and
- the individual must be given the express opportunity at the time of firsts contact to request not to receive any further direct marketing materials.

It will probably be impracticable to seek individual consent for most marketing lists.
The direct marketing exception is a substantial departure from the normal rule about use and disclosure. The price paid for this is:

- the need to maintain an appropriate data base entry that identifies those individuals who have asked not to receive direct marketing communications; and
- the need to provide a method for the individual to "opt-out" of the marketing list.

If a request is received to stop sending direct marketing communications, then you probably may insist upon reasonable identification procedures to ensure that the request is genuine. However, you probably cannot insist that the individual conform to any particular method of submitting the request. You may not impose a charge on the individual for honouring his or her request to opt-out.

4.4 Consents

In general, personal information should not be used for a "secondary" purpose except in exceptional cases. One of the exceptions is that the data subject has "consented". Consent may be either express or implied.
Care must be taken in relying on implied consent. In Turner v Royal Bank of Scotland,[4] the English Court of Appeal considered implied consent in the context of bankers' references. It held that there could be no consent for a practice that was not known to the general public. In the case under consideration, it was relevant that the practice was kept secret by the bank. See Tyree [2] for a full discussion of the case.
We can also expect to see the notion of express consent tested. The mere fact that a customer "consents" to practices located in the fine print is unlikely to be "consent" for the purposes of the Act.

4.5 Dual regulation

Credit providers will remain subject to Part IIIA of the present Act which regulates credit reporting. The interaction between the NPPs and Part IIIA is by no means clear. Is information "derived from a credit report" subject to the restrictions of Part IIIA even though the very same information would be subject to few restrictions under the NPPs?
Further, it is not clear how the NPPs interact with the Tournier duty of confidentiality.[5] For example, the NPPs clearly permit "personal information" to be disclosed to a "related company".[6] Case law has said that such disclosure is a breach of the Tournier duty.[7]

---

[4]English Court of Appeal, No 1998/0523/2
[5]Tournier v National Provincial and Union Bank of England [1924] 1 KB 461; the better view is that the Tournier duty also applies to building societies, credit unions and other ADIs. See Tyree, [1].
[6]Section 13B. Note, however, that the purpose of collection runs with the data: NPP2.2.
[7] Bank of Tokyo Ltd v Karoon [1987] AC 45; Bhogal v Punjab National Bank; Basna v Punjab National Bank [1988] 2 All ER 296.

4.6 Transborder data flows

In addition to the NPP restrictions on the use and disclosure of personal information, NPP9 adds additional requirements if the information is to be transferred overseas. The principle rule is that data is not to be transferred unless it is reasonably certain that the receiving organisation is obliged to treat the data according to rules that are similar to the NPPs.[8]

This rule works in connection with the "long arm" jurisdictional rule to permit transfer to related companies. Such companies are subject to the NPPs by s5B.

4.7 Action required

If your organisation is subject to the legislation, there are certain preparations which should begin immediately. Most importantly:

- you must have a policy on the handling of personal information;
- you must ensure that your policy complies with the NPPs or any applicable code;
- you must prepare a document which clearly expresses your policy;
- the policy document must be made available to anyone who asks for it;
- you must ensure that your systems can provide information to any person about the information your organisation holds;
- your systems must be able to provide access to information held on that person and to accept corrections of incorrect information.

Many of the restrictions on the handling of personal information are subject to an exception where the person consents. You should review all of your forms to ensure that they contain necessary consents. You should instruct your staff on dealing with customers to ensure that the consents are understood and effective.

Reference

[1] Alan L Tyree. Does tournier apply to building societies? *Journal of Banking and Finance Law and Practice*, 6:206–208, 1995.

[2] Alan L Tyree. Implied consent. *JBFLP*, 11(1):35, 2000.

[8] There are other exceptions: see NPP9.