John Ozimek is both writer and long-term practitioner in the field of database marketing and data security. As editor of the *Journal of Database Marketing*, he strives to stay abreast of the latest developments in this field. As a regular writer and contributor to the *Register* and other national news outlets, he is fast gaining a reputation for asking awkward questions about the government's use of data and the internet.

Legal and Regulatory Update

This section of the Journal looks at marketing, data protection, technology and e-commerce issues, providing an overview of recent key legal developments in these areas.

Best practice for safeguarding personal details and maintaining customer confidence

John Ozimek

Journal of Direct, Data and Digital Marketing Practice (2008) **10**, 161–171.
doi:10.1057/dddmp.2008.33

When unauthorised cashpoint withdrawals were first reported, the transaction was most frequently taken as *de facto* evidence of customer negligence or fraud

Background

There is serious and growing concern by consumers in the UK about identity theft¹ and ID fraud. Both can result in significant personal loss: in the worst cases, individuals may be left penniless for a period of time while steps are taken to resolve disputes.

According to the Banking Code of Practice (2008),² ‘unless you have acted fraudulently or without reasonable care (...), you will not be liable for losses caused by someone else which take place through your online banking service’. Similar provisions apply to other services, such as cashpoints and card payments. The onus, in theory, is on banks to show a lack of care on your part.

But this is not the way it has worked in the past. When unauthorised cashpoint withdrawals were first reported, the transaction was most frequently taken as *de facto* evidence of customer negligence or fraud. Rather than receiving sympathy, customers were treated with hostility and on more than one occasion reported to the police.

Over the last few years, efforts to combat credit card fraud in the UK have been supported by the introduction of chip and pin. Figures from APACS³ — the UK Trade Association for Organisations delivering payment services — suggest that this move has had some limited success in reducing the incidence of credit card fraud.

Where it is harder to commit fraud by one means, however, fraudsters quickly turn to other approaches — some highly sophisticated — in order to hoax individuals into giving away personal details.

The general approach is the same. Different terms are coined for methods according to the channel of attack.

John Ozimek
39 Church Street
Deeping St James
Lincs PE6 8H, UK
Tel: +1 778 344271
E-mail: emcity@easynet.co.uk

- Phishing E-mail-based: typically, e-mails will suggest that recipients click a link through to a website in order to re-enter a password because their details may have been compromised.
- Vishing Phone-based: more sophisticated fraudsters tend to make use of VoIP.
- ‘Phaxing’ Fax-based.

Card fraud is reported as increasing 8 per cent between 2006 and 2007

CIFAS — the UK Fraud Prevention Service — reports an increase of c. 8 per cent year on year between 2006 and 2007 in cases of reported fraud.⁴

When it comes to advice to consumers, the official line is fairly consistent:

‘Never give out personal or account details to anyone who contacts you unexpectedly’.

Organisations that give this advice, or very similar, include British Bankers Association,⁵ Home Office,⁶ Financial Services Authority⁷ and Metropolitan Police.⁸

It would be hard to be clearer. As the Met explain in respect of vishing: ‘...callers pretend[ing] to be major companies... promoting new deals on financial products such as accident cover. The caller then asks for birth details, marriage and family details and bank account details’.⁹

All of this contributes to a growing wariness on the part of the public. If you hand your details over to anyone, it could be held that any subsequent misuse is down to your negligence. Far from being compensated, you could lose a great deal financially and then be blamed for being the architect of your own downfall.

Two observations put public concern into perspective. The first is a simple year-on-year count for the Telephone Preference Service (TPS) database (Table 1 and Figure 1). This shows a significant rise in the number of telephone numbers blocked to unsolicited callers. The reasons for this blocking change over time: at one time, for instance, ‘silent calls’ — where automated dialling equipment dials a number, but the call centre does not have enough operators to handle it — have been a major source of concern. Interpretation of these figures may also be made more difficult by the fact that they represent lines blocked, rather than individuals: as the number of people owning two or more phones increases, one would expect the absolute TPS numbers

Growing public concern

Rejection of telephone as a marketing channel

Table 1: Year-on-year count of TPS database — 2002 to present

	Number opted out	Increase (year on year)	Percentage increase
May 2002	2,033,094	N/A	N/A
May 2003	3,007,981	974,887	48.0
May 2004	4,855,925	1,847,944	61.4
May 2005	8,307,476	3,451,551	71.1
May 2006	12,649,665	4,342,189	52.3
May 2007	14,714,840	2,065,175	16.3
May 2008	14,783,477	68,637	0.5

Source: TPS

Figure 1: Year-on-year count of TPS database — 2002 to present
Source: TPS

Public turn the tables on cold callers

to increase. While these figures are not quite the picture of unalloyed doom and gloom that they might be, they do not paint a very encouraging picture for the telemarketing industry.

The second observation is anecdotal, and therefore needs to be treated with care. That said, insofar as increased incidence in a particular form of anecdote may serve to highlight a new social meme, it is evidence that trend-watchers need to be aware of.

This is the ‘story’ of how individuals have reacted to cold callers. Over the last couple of years, it has been more and more common to hear of individuals claiming to have ended a particular cold call by demanding that the cold caller provide evidence of who they are. In other words, they have turned the tables in respect of the immediate power dynamic behind the call.

Earlier this year, a group demanding changes to the way in which large organisations work was given an audience on Radio 2 to put forward their point of view: they raised this specific point in respect of how consumers were meant to tell when a large organisation was genuinely contacting them.

Separately, the concept of greater customer control over how and when they are contacted has been written about widely over the last decade. It has been an emerging theme of CRM. This ranges from the simple ‘vanilla control’ — where companies claim to delegate greater control to their customers — while in practice carrying on much as before, to genuine delegation of control: for instance, giving customers the ability to edit their own personal information, as well as determine the time and manner in which they may be contacted.

Issues

Key issues are as follows:

- ID theft, leading to a rethink by customers as to how and when they interact with organisations
- resistance to existing supplier-oriented business practices
- growing pressure from customers for far greater control in their interactions with suppliers
- long-term risk that outbound calling may cease to be a viable channel of communication.

For companies, this presents a stark challenge. Their current approach to doing business is increasingly out of touch with how customers wish to do business: it can appear insensitive and, in the worst cases, to actually aid criminal behaviour.

Nonetheless, although this stems from a negative, it is also opportunity for those organisations that manage to resolve this demand in ways that appeal to customers.

Approach

Bad practice in action

This paper is not based on formal research. Rather, it draws upon a long and growing list of case studies in this area maintained by the author, in order to illustrate poor practice. Each of the instances documented below occurred in the last 12–18 months.

Although each instance is a one-off report, it is reasonable to assume that they are examples of a campaign that has been approved by the organisation in question, and — if the organisation was who it claimed to be — that it is typical of their behaviours and attitudes towards their customer base.

In each case, steps have been taken — by contacting the organisation concerned — to confirm whether the behaviours identified are or may have been carried out by the organisation.

Case studies

BT takes the prize for non-compliant marketing

BT: Conversion to direct debit

By far the worst example in our list. A BT subscriber received a call from a BT call centre. The caller talked about ‘good news’ if the subscriber was prepared to switch to direct debit.

The subscriber slowed the call down, inquired as to what information they were likely to need to divulge and, on being informed that bank account details would be needed, requested that the BT operator ‘prove’ that they were from BT.

This they eventually attempted by reading to the subscriber details from their most recent phone bill.

Unfortunately, since the subscriber had refused to provide sufficient details for personal identification, this was most likely a Data Protection breach: information was being disclosed without having validated the identity of the person to whom it was being disclosed.

The subscriber terminated the call. Subsequently, they attempted to register a complaint and to raise the case with the BT Data Protection Officer. Neither course of action was very successful due to what they described as the ‘labyrinthine’ nature of the BT call centre environment.

Corporate culture out of step with changing attitudes

Learnings

It is hard to know where to start with this case, as it appears to be a catalogue of poor practice from start to finish. It is particularly significant in that it is carried out by BT, the UK national telephone operator.

In seeking corroboration for this practice, the initial response from BT was that it was perfectly acceptable to phone out in this manner, so long as sufficient ID checks were carried out. The ID checks in question appear, however, to have been checks on the ID of the call recipient.

The idea that BT would go on to obtain bank account details flies in the face of all official advice given and sets a very poor example for other companies in this field.

Attempts to negotiate the maze that is BT Customer Service are talked about more widely as something that individuals would rather not do. It is likely that this is part of a wider issue in respect of over-automation of a highly complex process.

The inability to link to a Data Protection Officer is a serious failing, although oddly enough — according to the Office of the Information Commissioner — not in itself a breach of any principle.

The case appears to illustrate a corporate culture that has not taken any account of changes in public attitudes to outbound calling or public concerns over ID fraud. It is significantly bad practice and a PR disaster waiting to happen.

TV Licensing Renewal¹⁰

On the renewal date for their television licence, a viewer received an outbound call from TV Licensing. The caller explained that the viewer could renew their licence over the phone, using a credit card if they wished.

When the viewer questioned how they could know that the caller represented who they claimed to represent, the caller explained that they would provide some personal data to the viewer that ‘only they could know’, including the last four digits of the credit card that they had used to pay the licence with previously.

‘Helpfulness’ could lead to customer data loss

Learnings

This is outwardly better than the BT case, but only apparently so. The proposition being advanced to the caller is that the caller will ‘prove’ they are who they say they are by feeding them certain tidbits of personal information. Once they have done this, they will then seek to elicit further information back from the caller.

The difficulty here is that even supposedly confidential information is not that confidential. Investigators have estimated that the key security questions asked by many banks — postcode, date of birth, mother’s maiden name — could be obtained for a significant proportion of the population within minutes from the internet.

**Mobile phone market
a hotbed of poor
practice**

Provision of the last four digits of a credit card number is outwardly more secure — but since enhanced security in the credit card industry, this is all that is displayed on most credit card slips anyway. In the past, ID fraudsters could obtain credit card details quickly and easily just by raiding an individual's rubbish: credit card numbers were printed in full on discarded slips and many individuals just threw slips away with little or no attempt to obliterate the numbers.

Since this has changed, a fairly obvious extension of fraudulent activity is to use what information remains (last four digits) as a means to extract the full card number. Ironically, many individuals feel more secure about discarding credit card slips because only the last four numbers are printed — so making themselves more vulnerable to 'vishing' attacks that would sound little different from the approach detailed here.

Vodafone

At or near the contract renewal date for a subscriber contract, a call was received from an organisation purporting to be Vodafone. No attempt was made to prove that the caller was Vodafone.

Instead, they moved quickly into a series of identity checks in respect of the individual being called. When asked the purpose of the call, an explanation was given that this was to assist the individual in finding the best renewal package. When asked to 'prove' their own identity, none was forthcoming.

Learnings

This is very similar — at least at the outset — to the BT case. It is a phone company calling out, unable to verify its own identity, but expecting the call recipient to provide information to prove that they are who they say they are.

It does not quite reach the BT standard of badness, because once it becomes clear that the call recipient is not going to play ball, the call is terminated. Nonetheless, it is indicative of an attitude that appears to have completely ignored the public statements of government and industry bodies in respect of giving out personal information.

Discussion

The case studies above appear to illustrate a growing clash of culture and attitude between two different aspects of the commercial world. On the one hand, there is ID fraud, consumer concern about that issue and the advice from a range of official bodies, including government, that you should NEVER divulge personal or banking details to anyone who phones unexpectedly.

This is underlined by a banking attitude that negligence on the part of consumers can result in them failing to make good losses, together with some high-profile headline cases where the fact of fraud has itself been interpreted as indicating that some negligence took place.

A legal bonanza in the making

Meanwhile, large organisations — including some of the UK's largest providers of telecommunications services — continue to make outbound calls and solicit personal details as though nothing has changed.

This feels like a legal bonanza just waiting to happen. For instance, it would not be too far-fetched to imagine a consumer who unwittingly gave away banking details over the phone — and was subsequently refused compensation — suing their bank and calling BT in witness to what is considered 'acceptable practice'.

The court would then be required to determine whether consumers should listen to government and official advice, or simply respond to what is current accepted practice in the UK telemarketing industry.

It is not within the scope of this paper to pre-judge how such a case might turn out. It is the author's contention, however, that the onus is really on business to come up with better practice.

First, because of the potential for a PR disaster. Consumer affairs programmes are very keen to highlight phone scams and to expose the perpetrators of such practices. It is not hard to imagine a more creative researcher eventually drawing the link between what large organisations are doing and what the fraudsters are doing.

Secondly, because there are serious ethical issues implied in organisations doing nothing to change existing practice when, as suggested below, there are solutions that marketing departments can put in place. Continuing failure to address this issue suggests a preference to put consumer livelihoods at risk, rather than to adopt practices that are designed to support customers.

That's sharp practice — and sooner or later, sharp practice has a habit of rebounding on those who commit it.

Towards best practice

One obvious area where practice could — and should — improve lies outside the scope of this paper. This is within the banking industry itself.

Research suggests that the scale — and scope — of fraudulent activity is limited by the speed and efficiency of a bank's response. The existence of easily identifiable fraud hotlines, comprehensive training of staff, so that they are instantly aware of what action to take/where to refer a fraud query to are steps that can assist the wronged customer as well as limit potential losses for the bank.

In addition — as a simple matter of customer care — banks should consider how they treat individuals who claim to have been defrauded. It is always possible that the claim itself is fraudulent. But until that is proven beyond reasonable doubt, the complainant should be treated with courtesy and sympathetically.

The alternative is to deepen the upset for genuine victims — and again, to set up potential PR disasters at the point the victim proves their case. In the worst instances, hostile treatment of fraud reports can turn a victim into an enemy: someone who actively works to generate adverse publicity for your organisation.

Organisations ignore ethical considerations at their peril

Victims of fraud need extra care

Don't make enemies

Those familiar with the Loyalty ladder would be well advised to add this category as a bottom rung. Before Prospect, Customer and Advocate comes Neutral (individuals who have no interest or opinion at all about your products) and Enemy (individuals who have some highly negative belief about the products you sell). While these are most commonly found in respect of products with political associations (produced by regimes that are oppressive, environmentally unfriendly, animal rights, etc), they are also associated with instances where an individual perceives — rightly or wrongly — that they have been treated badly by an organisation.

Telemarketing companies need to take on board a similar lesson, which is that they should have easy-to-access routes into the company for individuals wishing to check that a phone call genuinely came from them. If a customer is worried that they may have been targeted for ID fraud, they can have their minds set at rest — or their anxiety levels increased — by a simple confirmation — or denial — that they have just been targeted by the organisation in question.

This would not only be good for customer relations. Where such a facility existed, and a company was suddenly alerted by several people to a campaign they knew did not originate with them, they should be able to alert police and customers to it before further damage was done.

For telemarketing companies and organisations that wish to make use of outbound telemarketing to make a sale, the current climate is an unhappy one. Certain details are necessary to complete a sale.

The best advice is for prospects never to hand out those details unless they can be sure that the organisation in question is who it claims to be.

There are a number of possible solutions within the confines of Business as Usual.

- *Encourage callback*: clumsy, but if managed through a publicly available free phone number, capable of maximising take-up. In that this approach would insert a delay between initial decision to purchase and final confirmation of purchase, it is not ideal.
- *Introduce a secondary channel*: essentially, carry out the sale on the phone, but send out either mail or e-mail on which customers can confirm or add key details. Again, not ideal, because it adds an extra step to the process and it is open to abuse.

Quick fixes are not ideal

The real difficulty with both these approaches is that they continue to force customers to work in modes that suit the supplier. They increase safeguarding to some extent, but do so at the expense of seamless service.

No doubt they represent a short-term solution for some organisations, but it also seems likely that they will be superseded because they are cumbersome. Customers will opt, in the end, for the system that makes them do the least work.

The one solution that feels as though it is likely to be inevitable, in time, is the creation of an independent means of verifying that an

Organisations may one day need their own passwords before doing business

organisation is who it claims to be. That, in turn, would require the organisation to store certain details (code words or tokens) that are specific to its relationship with a particular customer.

These details would need to be taken in parallel with other permissions — in fact, in time, could come to stand in for permissions data. That is, when an individual first becomes a customer, best practice already suggests that an organisation should obtain consent to contact that individual — and agree on what channels can be used for contact.

The process could be extended, so that at this stage in a relationship, an organisation would also agree with a customer on what means they would use in future in order to identify themselves.

For instance, if I agreed with BT that they could call me — but that before any conversation commenced, their operator would play back to me a password that I had previously given to them — then this would go a long way in eradicating concerns over who they were.

One complication is that this would become unmanageable if applied to multiple organisations. If the password chosen is sufficiently complex, however, there is no reason why the same password could not be used for ‘any organisation I wish to empower to call me’.

Clearly, there is a risk that the password could be compromised: if employees of organisation X stole the password information and then phoned up pretending to be representatives of organisation Y, it would make fraud all the more easy. The person on the receiving end of the phone would have enhanced confidence in the *bona fides* of the caller — and perhaps be less inclined to question their need for extra details.

In such cases, however, it should be fairly easy for the individual to argue that they had not been negligent — and if banks wished to pursue anyone for negligence, it would have to be the organisation whose security was compromised.

Is this approach too much of an imposition? Undoubtedly, some consumers will see it as such, since it is a requirement for them to remember ‘yet another thing’ in order to manage their daily lives.

In the end, though, something has to give. Organisations would like to continue calling individuals and, as part of the conversation, to extract personal information. At the same time, they make it quite clear that individuals who give away information to the wrong people may be liable for any losses that result.

That is a major disincentive to doing business by phone — as, too, is any system that places too great an administrative burden on the customer as a requirement for doing business.

None of the solutions set out above are ideal, but it is not the aim of this paper to come up with a definitive solution. Rather, the aim is to highlight the problem and hope that the business community can come up with solutions less cumbersome and more elegant than the obvious ones discussed here.

If the thought of thousands of different organisations all having to add personal password facilities to their software sounds like a nightmare — it is not. For most systems, it would be a fairly minor

OpenID — the way forward?

Organisations that do not address the issue of customer confidence seriously may soon find themselves very short of customers

modification. Alternatively, this is an area where the use of ‘OpenID’ technology could be appropriate.¹¹

One area where elegance is becoming much more ‘the norm’ is online. Here, the issues raised above have begun to be addressed from the organisational side of the fence. That is, there is a growing demand for verification that an individual is who they say they are — or that they are at least the age they claim to be — before they can trade.

Traditional solutions involve e-retailers holding large amounts of personal details about the individual: customer databases with sensitive personal details. These are all very well when it comes to maintaining an ongoing relationship, but may be overkill when it comes to the simple question of whether an individual is old enough to buy a 15-rated DVD online from a site they may never wish to visit again.

A typical solution to this type of problem is the one put forward by the Information Card Foundation¹² — a consortium that includes Equifax, Google, Microsoft, Novell, Oracle and PayPal. They are creating ‘Information Cards’: different cards can contain different levels of information and can be used to log in to different websites instead of using a user name and password. Some may contain just a user name and password; others address information.

The important point about this approach is that the sensitive information is held once on a single database rather than repeated a dozen times on individual site databases. Once signed up for a given level of security, customers do not need to repeat the process.

This is a very similar approach to OpenID — a project based on open source solutions. It provides individuals with a single source of ID information that is held independently of any single commercial organisation.

In fact, the card element to the above proposals may be unnecessary. NetIDme¹³ is a UK-based company developing age-verification systems for content providers such as the BBFC (British Board of Film Censorship).

Their system works by creating a token — in practice, a cookie — that a user drops automatically onto any website from which they wish to make a purchase. The token is created initially from an assembly of personal information, but once the token has been created, the original information is then disassembled again.

None of these systems are perfect: none pretend to be. One of the greatest critiques of systems such as these, where key data are held in one place, is that it is as vulnerable as the security of the weakest organisation in the chain. Once the security is compromised, an individual will be vulnerable to attack on a number of fronts.

This, however, possibly ignores the fact that individuals are vulnerable anyway. Criminals are always developing new ways to hack or exploit data. So the debate will always devolve to a question of balance between conflicting risks.

While the last section has focused on how organisations can identify individuals in ways that are less onerous to the individual and at the

same time more secure, it should be clear that the same technological approaches should be applicable the other way round.

Online tokens or ID systems to verify that an organisation is who it says it is are definitely one way forward — and only time will tell whether there is sufficient consumer demand to put them in place. Given the growing trend for individuals to combine phone and internet when doing business, it is possible that an online solution will go some way towards resolving phone security issues as well.

Conclusion

The purpose of this paper has been to highlight a growing problem for organisations that need to elicit information from individuals as part of their outbound (tele)marketing. Customer resistance to traditional ways of doing business is growing — and good secure systems for safeguarding customer data are not yet in place.

This paper does not provide neatly packaged solutions; it does, however, begin the debate on what such solutions might look like — and suggests that the time has come for organisations to refocus their trading practices in a more customer-centric way.

I hope that this issue will strike a chord in some marketing departments — and may form the basis for an emergent best practice in this area.

References and Notes

1. Silicon.com special Report. (2008), <http://www.silicon.com/research/specialreports/fulldisclosure/0,3800014102,39225528,00.htm>.
2. Banking Code of Practise. (2008), published by the British Bankers' Association, http://www.bba.org.uk/content/1/c6/01/30/85/Banking_Code_2008.pdf.
3. APACS: Card Fraud Facts and Figures, http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html.
4. CIFAS Fraud Trends 2007, http://www.cifas.org.uk/default.asp?edit_id=790-57.
5. How to beat identity fraud, published by the British Bankers' Association, http://www.bba.org.uk/content/1/c6/01/11/11/BankFact_how_to_beat_id_fraud.pdf.
6. Home Office leaflet on ID Theft, <http://www.callcredit.co.uk/download/Home-Office-Identity-Theft-Leaflet.pdf>.
7. FSA Site, http://www.moneymadeclear.fsa.gov.uk/guides/staying_safe/staying_safe_against_scams_step_1.html.
8. Metropolitan Police, Fraud Alert. (2006), <http://www.met.police.uk/fraudalert/news/phishing2.htm>.
9. *Ibid.*
10. TV Licensing reviewed this case history and confirmed that it is an accurate representation of their practice. They, however, added that if a customer, who has received an outbound call, questions whether the call is from us, they can use 1471 to call back on an 0800 number which will connect to the main TV Licensing customer service line.
11. For further reading on OpenID: <http://openid.net/>. For a list of current providers of OpenId, try <http://wiki.openid.net/OpenIDServers>.
12. The Information Card Foundation, <http://informationcard.net/>.
13. NetIDme, <https://www.netidme.com/Welcome.aspx>.