Culture

Identifying the problem

Peter Massey and Tim Kitchin have both professional and, unfortunately, personal experience of dealing with identity theft. They argue that elimination of the problem is virtually impossible, but effective control depends on adopting a different approach.

On the assumption that everything that happens in America happens here eighteen months later, Britain seems set for a nuclear explosion in identity theft, with the potential for lingering contamination in the economic system. Eradicating this is probably impossible at this stage, but control is a realistic aspiration, provided that identity handlers can *sympathize, empathize,* and *operationalize* to address the growing identity anxiety.

Managing identity theft is as much about embracing consumer psychology as it is about preventing the crime. To achieve this, financial services organizations should act more humanely at the customer interface; provide service solutions that recognize the psychological trauma involved; and move beyond mere technology adoption to operationalize identity theft prevention and response processes consistently and reassuringly across all channels. They must systematically remove their customers' grounds for mistrust.[1]

In Britain, of course, criminals are playing catch-up with America. There, identity fraud has been estimated at $50 billion by Benchmark Group (see box), whereas the British government puts the problem at "just" £1.3 billion over here in the same period. But it is the knock-on effects on customer confidence that are ringing alarm bells.

Hidden costs

The direct cost impacts are just the tip of the iceberg. Second-order effects include reduced service use by affected customers; increased incident-handling costs; increased internal compliance activity and cost[2]; significant technology investment; and some business process re-engineering. We estimate these effects at between five and ten times the direct impact.

However, the real danger lies beyond even these identifiable costs. There are three big mid-term effects:

- The threat of **increased regulation**, requiring much greater transparency from information holders and giving consumers rights of access and even prosecution against lax data-handlers. This is already coming home to roost in America, not least because identity theft has caught the attention of New York's combative Attorney General, Eliot Spitzer.
- The threat of **customer self-protectionism**. As consumers shield themselves from attack, this will lead to reduced cross-sell through the rejection of intrusive marketing (for example, telemarketing, direct marketing and face-to-face) and also reduced use of self-service channels such as on-line and tele-banking. Already, TPS and MPS[3] opt-out rates are approaching a quarter of homes, and almost half of telephone subscribers are now ex-directory.
- Perceived untrustworthiness, leading to a threat of **reputation breakdown**. The personal experiences of one of the authors indicate that some organizations may be well aware of systemic fraud but are unwilling to take action against business partners that are consistently "leaky". At present, such decisions do make strict commercial sense, but the dynamics can soon change. A balloon of fear is inflating under the kitchen table. When it expands beyond a certain point, all the financial crockery will come crashing to the ground.

THE AMERICAN PICTURE

In the United States in the last few months:

- Two major information brokerage companies* have admitted that data files of over 455,000 consumers have been breached.
- One of the world's largest financial institutions, Bank of America, confirmed† that back-up tapes containing personal data on 1.2m accounts were missing.
- Federal authorities confirmed an investigation into the electronic hacking of eight million credit card accounts from the processor of credit transactions for MasterCard, Visa, Discover and American Express.
- A popular shoe store chain, DSW Shoe Warehouse, admitted that customer credit information had been stolen from over a hundred of its stores.
- According to MillersMiles.co.uk, 40% of targeted Citibank customers fell for a phishing scam in 2003 and supplied their financial identity details to an organized criminal network. Even sophisticated consumers can be fooled.
- Approximately 180,000 Mastercard holders will soon receive notification that their personal information may have been stolen in a data breach at Polo Ralph Lauren.‡

* ChoicePoint, Inc and LexisNexis. See consumeraffairs.com/news04/2005/choicepoint and consumeraffairs.com/news04/2005/choicepoint_schumer.
† See consumeraffairs.com/news04/2005/choicepoint_bofa
‡ See consumeraffairs.com/news04/2005/gm_mastercard.

According to research conducted by YouGov for Glasshouse Partnership[4], 17% of British consumers have direct or indirect experience of identity theft – ranging from 13% in Scotland to 28% in London – and only 46% now feel their identity is safe. In terms of responsibility for fighting identity theft, 86% of respondents said banks should do more, with the government second in line. Identity anxiety is clearly on the rise.

Interestingly, those who had experienced identity theft (a large number, don't forget) were twice as likely to reject personal blame. Having experienced the reality first hand, victims see how powerless they are; how easy it is to utilize a stolen identity, and how disconnected and unaccountable the support and reparation processes can be.

At present, corporate communication around identity theft is confined to public education, effectively shifting the burden of responsibility upstream to the individual. But as the phenomenon becomes more widespread, the willingness to accept that citizen-level solutions are sufficient will tail off. Attention will shift both downstream, to more stringent authentication of identity in use, and also right back to the source – to the integrity of those root documents and shared databases – one of the key practical issues at the heart of the identity card debate.

More technology?

In an environment in which half a million driving licences are lost or stolen each year, would increasing centralization actually serve the public good, or just increase the risks? Once you have someone's driving licence, you're off and running in fraud terms. So how much more secure would identity cards be?

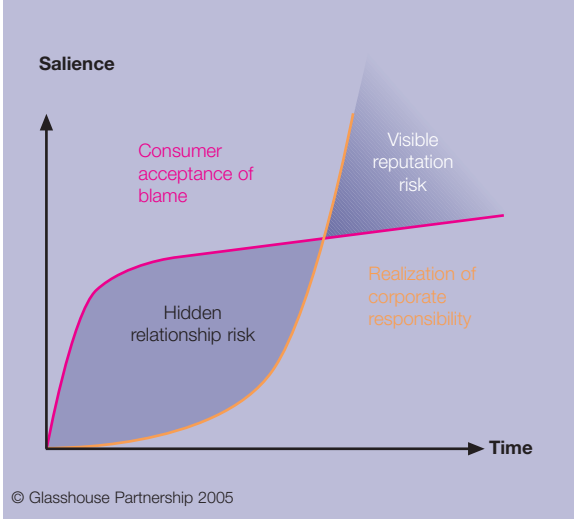
Our research showed that just 23% of people trust the government not to abuse their personal details. And just 5% would trust the private sector to administer such an identity database. Beyond even the personal liberty debate, there is a real argument yet to play out around the effectiveness and reliability of particular technology solutions. Trusted organizations that hold extensive personal data, such as Royal Mail, BT and Experian, have an opportunity to play a big role as personal information brokers in a more anxious world, if they can persuade consumers that they are both transparent and accountable in the way they use that data.

Those who had experienced identity theft were twice as likely to reject personal blame.

At the same time as consumer self-blame diminishes, the scrutiny and criticism of the protection measures taken by banks, retailers, police and government will increase. These organizations face a TINA scenario – *there is no alternative* – of increased reputation risk. As scepticism grows and sophistication increases, they must act – see Figure 1.

In this context, the banks are on the horns of the dilemma between delivering simplicity of service and

FIGURE 1: THE GROWING REPUTATION RISK



effective customer protection, but must ask themselves whether they are doing enough. Is there actually a fast and simple solution to identity anxiety, grounded in basic principles of communication and service?

At a recent Glasshouse seminar[5], Peter York, the social and brand commentator, accused banks of being autistic – displaying the same corporate symptoms as those individuals who are completely self-absorbed and who have a reduced ability to respond to or communicate with the outside world. In the words of The John Lewis Partnership, he said, it's not about how you prevent a problem; it's about how you recover. Or, to pin it to a fairly reliable statistic, the loyalty of a customer who has complained and been satisfied (as measured by the Henley Centre) can be as high as 91%, compared to 59% for customers who have had no cause for complaint.

Psychological problems

The loyalty and disloyalty pendulum for customer service is directly related to the emotional risk involved. Win–win and lose–lose outcomes are much more likely to occur, with little room for compromise. Win–lose is an unlikely outcome when the stakes are so high. The authors' own fraud experiences suggest that account closure is a reasonable and common first-response by a customer to a poor experience of a full-on identity breach.

We certainly don't believe banks are autistic, but we do think their existing behaviour shows evidence of classic "ego protection", and that resolving individual customer experiences must be a first priority.

We can think of corporations in the psychological language of Freud. In a corporation, the role of the corporate ego is to arbitrate between the needs of the id – the "pleasure-seeking", short-term, profiteering part of the organization[6], and the needs of the super-ego, the moral conscience, which recognizes the need for transparency, governance and self-control – see Figure 2.

Of course, the super-ego is powerful force for restraint, but the ego has several helpers – known as defence mechanisms – in this struggle for equilibrium. In the identity theft context, within such a charged emotional environment, all the classic corporate psychology defences can be observed.

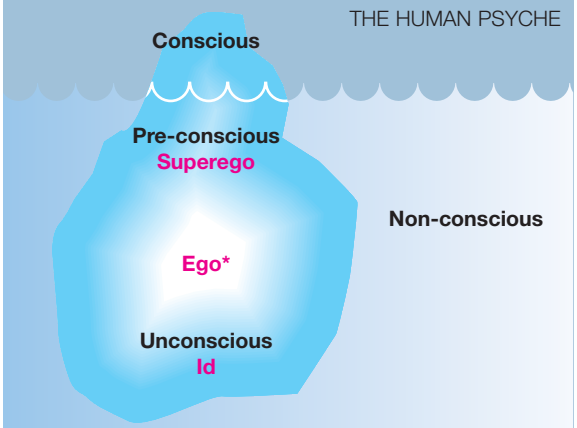
However effective the corporate defence mechanisms are, though, ultimately the both sides have to face up to reality and find a compromise, grounded in mutual need, not repression.

The reality of the identity theft situation is undeniably complex. All organizations face a quandary in maintaining consumer trust. The more they talk about it, the more fearful people may become. On the other hand, if they let the issue escalate, they may stand accused of complacency or even negligence. Realistic reassurance and genuine responsiveness are required.

We believe the answer lies is a "back to basics" approach. Fix this at the front-line. Seek to do what you as a customer would expect, and to make your actions as explicit as possible – publicly, privately and personally.

In summary, dealing with identity theft is no different to dealing with any other relationship-critical issue. Get the basics right, and everything else will follow.

FIGURE 2: FREUD'S ICEBERG METAPHOR



CLASSIC CORPORATE DEFENCES

Denial – Problem, what problem?
For example, failure to identify and report the full extent of identity theft within fraud and bad debt.

Displacement – It's your problem, not mine.
For example, using new technologies or trade education to transfer the onus onto retailers or customers to clear up the problem.

Intellectualization – You wouldn't understand; it's terribly complicated.
For example, investing in authentication processes, spam-prevention technologies and internal identity management systems at the back end, whilst failing to inform front-line staff of the fraud escalation procedure.

Projection – You are fat, I am big-boned.
For example, banks offer plenty of advice to consumers but rarely share what they are doing to clean up their own systems.

Rationalization – If you think about it, we have no choice.
For example, clinging to the dogma that "customers wouldn't accept greater protection". Well, Glasshouse's research shows three in five people would welcome a slower – and even a more expensive – process for the benefit of greater security. Being open to the idea and adopting it are very different in practice, of course, but this level of sensitization undoubtedly creates new marketing opportunities for responsive operators.

Reaction formation – I can't stand smokers since I stopped myself.
For example, Capital One's brave decision to offer its customers an identity protection plan as a USP – seen by many as "too much, too soon", and by some media commentators as lacking real usefulness.

GETTING THE BASICS RIGHT			
Sympathize	**Public** (Public relations)	**Private** (Process design)	**Personal** (Customer interaction)
	Establish a process for tracking and monitoring the state of public concern. Integrate identity theft into corporate social responsibility, governance and reporting priorities.	Understand staff attitudes to identity theft prevention. Institute appropriate controls. Attack your own systems from an identity theft standpoint. Profile the vulnerabilities and risks of escalation.	Identify root causes for each customer contact. Develop agreed escalation procedures, call scripts and customer-handling protocols.
Empathize	Develop communications to share the solutions you are adopting to protect yourself and your customers. Review brand content around identity theft. What advice do you offer, through which media? How consistent are you? Are you tracking take-up and download? Prepare holding statements and crisis response procedures in the event of a mass hack.	Mystery-shop your organization from a fraud victim's standpoint of high vulnerability. Ask yourself at each moment of truth whether the customer's trust has increased or diminished. Create a picture of the trust-flow. Review the cross-sell/on-sell processes for self-protection products and value-added services – and ensure that the value goes to the customer as well as the company.	Develop consistent incident follow-up procedures. Ensure all relevant departments understand their role in the care process: legal, fraud, customer care, billing, marketing and so on.
Operationalize	Enact a communications campaign that recognizes corporate vulnerabilities and addresses the causes of consumer anxiety.	Ensure one individual has ownership of the identity theft problem. Build an identity theft process from the customer's perspective.	Implement an identity theft value-improvement strategy to reduce corporate risk by improving the customer experience.

Ensure that your organization is genuinely listening to the voice of the customer, through all channels. Ensure your public stance, private behaviour and personal contact are aligned. If not, prepare to manage the risks. Once these **basics** are in place, move on to:

Brilliant basics. Redesign the customer management process end to end – from the customer's perspective. Monitor inconsistencies and unnecessary in-bound contacts, and eradicate them. Remove the sources of mistrust.

And then **close the loop**. Set in place processes to learn from pattern changes and to continually improve and refine.

The challenge could be accurately summarized by one of the respondents to Budd's 2005 *Fast + Simple* customer service excellence survey[7]:

> Managing identity theft is about turning an improved customer awareness attitude into actual improvements in service that customers can feel.

It is certainly time to stop doing dumb things to customers. □

Peter Massey is CEO of Budd UK and Tim Kitchin is a partner at Glasshouse Partnership

[1] Gide's maxim that the lesson of history is that the lessons of history are forgotten certainly seems to apply to financial services. The banks' initial responses to emerging problems with ATM fraud were (i) to deny that any problem existed; (ii) to blame it on customer deception; and (iii) to deny liability by blaming it on customer carelessness in disclosing their PINs and other personal information. Only much later did they recognize the structural limitations of the "foolproof" systems and the ease with which organized crime could apply both technology *and* an intrinsic understanding of customer psychology and behaviour – and it was only at this latter stage that the banks were able to introduce an effective containment strategy. Ed

[2] It is not just the direct financial cost that is important here, but also the "corporate opportunity cost" – the lost value of things that executives and departments are *not* able to do because they are chasing the compliance dragon. Mike Rake, the chairman of KPMG, argues (*Sunday Times*, 1 May 2005) that "… the amount of time a board spends on governance rather than strategy has become disproportionate". Ed

[3] The telephone and mail preference systems that allow people in Britain to exclude themselves from all UK-generated direct marketing and telemarketing activity. Ed

[4] 1,936 consumers were surveyed in March 2005 – see news at glasshousepartnership.com for more information.

[5] 17 March 2005.

[6] The "instinctive desire" of most organizations is still to make a profit first. The declared corporate desire may be different, but what matters to customers is how they are treated at the coal-face rather than how the glossy brochures tell them they will be treated. Ed

[7] See www.budd.uk.com/news