

EURIM
DIRECTORS ROUND TABLE 24TH NOVEMBER 2008

**An Irrelevant Overhead or Central to Survival ?
Setting the Information Governance Agenda:**

**Regulated Financial Institutions-
In the Eye of the Storm:
The role of banks in Information Governance**

Key Summary Points:

- i) Do not attempt to re-invent the wheel- build on what was done in the paper world and what is being done today in the eWorld ; to re-invent is very expensive/complex and takes a long time- today Society has neither the luxury of money or time.**
- ii) A durable solution is MUCH more than a Technology solution; for it to be truly interoperable and for liabilities rights & entitlement to be totally understood by all parties, it must span Policy, Legal and Operational dimensions aswell as the Technical piece**
- iii) Remain technology/vendor agnostic (ie Freedom of choice), but build upon existing open and mature standards- avoid proprietary lock-in, and minimize information actually held on an end-users credential.**
- iv) A durable solution must be global- and highly scale-able. Solutions which address a geographic area, an industry sector or a customer group are less likely to scale far beyond their confines. Multiple bi-lateral agreements cannot scale- furthermore unknown Risks can permeate through discrete "Islands of Trust".**
- v) Good governance encompasses freedom of choice for the end user. Where does the end-user place his/her trusted relationship, and what uses/applications can it enable, and what are the accompanying liabilities.**

To some observers and to those impacted by the turbulent events in the financial markets (ie all of us), it may seem perverse to submit a Paper to EURIM about Privacy, Authentication, Integrity, Accountability, Non-repudiability, Privacy, and other qualities which are historically associated with Banks/Financial Institutions- coming at a time of unprecedented difficulties in key areas of their businesses.

However, perhaps the timing is absolutely right for reasons outlined below.

Background:

Since Sumerian times over 8000 years ago through to their sophisticated structures today, banks have been in the business of risk management and risk mitigation. They have done this in 3 distinct areas- and generally speaking each of these areas have waxed and waned, but never all simultaneously- even today.

These 3 areas, all underpinned by mandatory strong "KYC" requirements, are:

- i) Credit/Deposit Risk Management- the accepting of deposits and the granting of loans .**
- ii) Trading/Capital Risk Management- using the Capital of the bank to trade in financial markets.**

iii) Operational/Transactional Risk Management- Moving value/financial instruments/money across dependable/secure clearing and settlement systems (both domestically and internationally) and managing the liability flows which accompany these processes/infrastructures.

This document is primarily focused upon (iii) above, which over recent years has generally played a lower profile role than the activities in (i) and (ii).

However given the well known current problems in categories (i) & (ii), banks and their customers are coming to see that their Operational Risk Management skills as increasingly important- and such “transaction management” businesses can produce steady reliable revenue flows- arguably preferable to the lumpy flows associated with credit and trading activities, as well as addressing the very real needs of their Customers to be able to transact business electronically in a trusted manner.

Thus the time is right for banks to step forward.

Payment systems:

Historically payment systems have evolved from very local practices of barter and bills of exchange into today's highly sophisticated frameworks, operating at both a domestic and an international level- with clearing and settlement systems increasingly executed in real time/at the click of a mouse (eg UK's Faster Payments).

These systems all share a common feature that makes them so effective- namely the member banks who form the channel from each system to the end-user, all sign up to a set of Agreements which define the dimensions, rights, entitlements roles and responsibilities of the system, and by extension the rights, obligations, entitlements and responsibilities of each end user.

These agreements are contractually binding on all parties, and are executed in advance- thus everyone knows exactly what they are, and are not, “on the hook for”. There is no room for doubt, and no “grey areas”.

These payment systems which are used by all of us whether in our individual or employment capacity, whether in the private or the public sector- are effectively woven into the fabric of contemporary life; to some extent, they are taken for granted- but without them, civilisation/society would grind to a halt.

To illustrate this, we all use the plastic card payment schemes as part of everyday life- they are all underpinned by just the sort of “RuleSet” as defined above- we take it for granted; it is part of the plumbing.

Building on these systems:

The era of ubiquitous and largely “free-to-use” electronic networks is now fully upon us- enabling massive amounts of information (well beyond payment information) to flow instantaneously- both locally and across borders.

Communications/emails which originate in the UK and are destined for an address in the UK may well be carved up/dissected many times, with pieces passing around the world only to be reconstituted a few seconds later in the Inbox of the recipient.

In such an environment, where privacy, authenticity, integrity and non repudiability of information is required, it is essential that a similar set of operating practices/processes and liability flows lie at the core of important electronic communications- exactly as has appertained in the payment world for many decades.

Regulation:

Financial Institutions are the most highly regulated sector of any National economy- and given the events of the past few weeks/months, that degree of oversight/regulation shows no sign of diminishing. Hence there should be a high degree of comfort on the part of both Public and Private Sector organizations in having Financial Institutions playing a pivotal role, under sets of pre-agreed contractually binding processes/procedures, in tightening up good practice, accountability (who authorised what and when) and audit trails- all essential to sound Information Governance.

i) Process Improvement, ii) Information Security & iii) Compliance:

These three dynamics should go hand in hand- in the past all too often they have not- now they are aligned.

In terms of Process Improvement, we are seeing significant demand for streamlining business processes, eradicating the dividing lines between “physical” and “financial” supply chains – moving to genuine “straight through processing” and simultaneously taking paper out of the system contributing toward the Green/Eco-friendly targets.

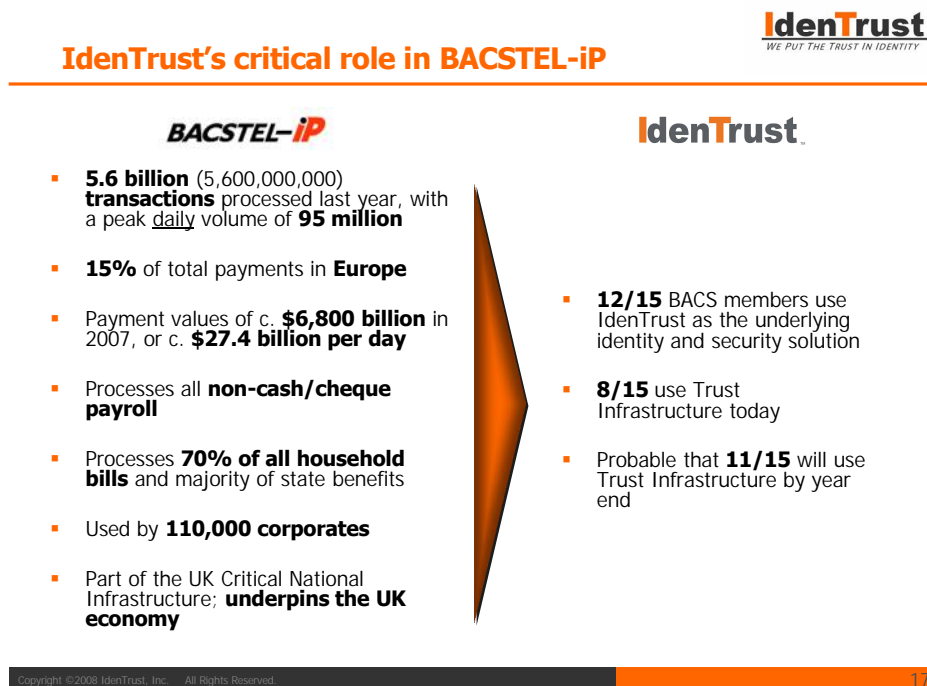
In Fraud/Information Security we are now witnessing a very substantial increase in “Customer-not-present” (CNP) fraud- this was highlighted most recently (8th October) by Nigel Evans MP Chairman of the All-Party Parliamentary Group on Identity Fraud; this in itself will force banks and their customers (public & private sector) to make much greater use of higher assurance solutions which are already available (and are being used)- the IdenTrust scheme being a perfect example.

With regard to Regulatory Compliance- by adopting such a Rules based approach, businesses can benefit by using digital signatures which are globally enforce-able

and cannot be repudiated- right down to the individual signer level, Thus leaving no doubt who signed/authorised/approved what and when.

Bringing this to fruition:

The success of the BACSTel IP migration of UK PLC's direct debits/direct credits from the antiquated system based largely upon 1970's technology, to a fully IP based modern platform is a real success story of which the UK can be justifiably proud. This migration was declared as mandatory by the BACS community of banks- they had to do it- the statistics below show just how significant it is.



Similar mandatory initiatives (eg the Public sector to require eInvoicing instead of paper), coupled with end-user driven initiatives (eg the management of Bank Mandates using electronic signatures)- place a degree of compulsion on organizations- meaning that system enhancements can and must take place, and the benefits can be measured.

Such initiatives can start with:

- i) Working with leading banks, identify Pain Points today.
- ii) Pick easy do-able Proofs of Concept/Pilots today which demonstrate the principle- thus minimising the risks associated with massive centralized projects.

These Pilots build on what is already in place; indeed past experience in this field is of enormous assistance in setting and executing on a genuine improvement of Information Governance.

Conclusions:

Heightened Information Governance is now a mainstream Boardroom agenda item in both Private and Public Sectors.

In seeking dependable solutions to this challenge, there is no need to reinvent the wheel; indeed in todays troubled climate “wheels” which already demonstrably work and are fit for purpose, should be embraced with alacrity and taken forward with a renewed degree of urgency.

Inactivity is simply not an option.

Proprietary and/or “point” (ie single purpose) solutions should be avoided; open standards and open networks are much to be preferred- and organizations must realise that it is not simply a matter of a Technology solution- good Information Governance requires a holistic approach spanning Policy, Legal, Operational dimensions aswell as Technical specifications- indeed in many ways the Technical piece is the easy one. It is in the Policy and Legal especially where the “devil lies in the detail”.

**John G Bullard
Global Ambassador
IdenTrust
London**

October 2008