BT Managed Fraud Reduction

Confidence in online business from stronger identity assurance
The BT Managed Fraud Reduction service

Intelligent fraud detection and prevention for online business

The BT Managed Fraud Reduction (BT MFR) service will reduce your organisation’s losses to due to fraud and fraud mitigation activity. It will detect and block suspicious transactions on your online applications, ensuring that only genuine transactions are permitted.

Fraud prevention is an arms race. As organisations continue to push business towards the less expensive web channels, fraudsters find ever more sophisticated ways to breach security and steal other people’s money and goods.

In the UK alone, during 6 months of 2008, online banking fraud rose by a staggering 185%. Fraudsters have become much more adept at mimicking bank and building society websites and 20,000 phishing attacks were recorded in that same period.

The majority of attempts to defraud retailers with stolen credit and debit cards will occur online in consumer sales, with criminals targeting any commodity they can sell on through the black market.

Online fraud is an industry in itself. Stolen debit and credit card details and financial account credentials are available to buy online. In a single year, Symantec counted over 69,000 distinct active advertisers of stolen financial material with 44 million related messages posted to underground forums. The potential worth of all the credit cards advertised was $5.3 billion, with a further $1.7 billion available from compromised bank accounts.

The challenge for any online application provider is to stand up to such a concerted challenge. Organisations need to minimise losses without compromising the genuine customer’s online experience by forcing the use of clunky authentication tokens, or blocking genuine transactions through over-cautious fraud prevention detection schemes.

Managed Fraud Reduction: a joint solution from BT and Oracle

BT, in collaboration with Oracle, has developed the BT Managed Fraud Reduction service as a secure, flexible and cost-effective solution to the problem of online fraud.

Our context-based, fine-grained risk analysis allows the service to make intelligent real-time decisions about the authentication and ID-verification criteria required to let a transaction proceed. Rather than simply blocking a transaction, the service automatically invokes ‘step-up’ authentication calls where extra validation is necessary.

This approach maximises the online completion of ‘good’ business – blocking only the most highly suspect transactions for offline analysis.

Uniquely, we integrate this service with BT’s world-class ‘URU’ identity verification system to provide extra assurance that the user at the other end of the transaction is who he claims to be.

By offering this as a convenient managed service, we provide the double benefit of allowing your organisation to reduce your fraud and your costs.

Sophisticated anti-fraud protection, 24*7*365

Using BT’s Managed Fraud Reduction service you can quickly and easily implement an intelligent, context-based fraud detection and prevention scheme for your current online applications – without having to dismantle your current authentication mechanisms.

The service will determine the risk associated with every customer transaction by examining the ‘context’ of the transaction with respect to the customer’s:

- typical online behaviour
- device
- location

- 66% annual increase in identity fraud incidents reported to a UK agency in 2007 (Source – Experian ‘Victims of Fraud Dossier Part IV’ 2008).

Customisable policies and rules are used to calculate the risk ‘score’ of a transaction. This score will then be returned to your online application, along with a full disclosure of how the score was determined and recommendations on how to proceed.

Most transactions will be genuine and will be allowed to go ahead straightaway. Some will have slightly higher than normal scores and might be dealt with by asking the user to answer a security challenge. Transactions with higher scores might require more stringent checks: the user might be asked to provide more personal data to be verified using BT’s URU service, for example, or a one-time-password required, generated via a token issued to your higher value customers and verified using the BT Managed Authentication service. In any of these situations, our adaptive, risk-based, context-checking approach gives each transaction every chance to proceed with only the most suspicious being finally blocked.

The service is on guard 24*7*365 protecting your organisation from bogus transactions at every point in your online application – from bogus account opening or registrations (with stolen credentials) to fraudulent in-flight transactions, such as transferring money between accounts or making a purchase from your online retail site.

The service can collate real-time transactional data from your ATMs and call centres and analyse this during the scoring process in order to spot cross-channel fraud (such as a change of contact details by telephone, immediately prior to a web transaction transferring funds to a new account.) External repositories can also be interrogated and included in the score calculation. For example, you might want to check your shipping records to ensure a customer has successfully received and paid for a number of high-value items before you agree to ship to an alternate address.

You will have full control over your own rules and policies which you can update in real-time, and you will automatically become part of our Fraud Intelligence Network, receiving early tip-offs on suspicious accounts, email addresses and IP locations.

Furthermore, when your genuine customers change the way they interact with your business, the system will ‘learn’ to recognise the new profile and let them transact as normal: incurring minimum inconvenience whilst providing maximum business and consumer confidence and protection.
Why use a BT managed service?

Benefits of the managed service

BT has extensive knowledge of deploying and operating identity and access management (IAM) systems. We have deployed IAM solutions across many market sectors and also manage the systems providing access to our own corporate information network for more than 100,000 employees.

BT has built the Managed Fraud Reduction service around the vision of offering a secure, shared platform. Sharing the platform amongst organisations substantially reduces costs and allows us to pass on significant economies of scale to our customers.

BT bases its services on the most innovative products in the marketplace. That is why we have partnered with Oracle to base our service on the world-renowned Oracle Adaptive Access Manager which delivers the next generation of risk-based evaluation, enabling real-time blocking of fraudulent access requests with unparalleled functionality, flexibility and performance.

- Our service is highly scalable and flexible, and thus able to meet anticipated future requirements.
- Our service has been designed to integrate easily with your organisation’s existing systems, processes, people and procedures.

Your organisation will benefit from lower total cost of ownership, faster deployment and less impact upon your own technical resources, as well as:

- **Associated services** – using BT’s Managed Fraud Reduction service enables you to take advantage of some of our other world-leading fraud reduction services, such as our URU identity verification service, or our Managed Authentication service which can provide simple strong multi-factor authentication for your applications. (If, however, you have your own equivalent services in place, then the service can integrate these with no additional effort.)

- **Reduced commercial risk** – our service provides clear commercial models providing transparent pricing plans, allowing predictable budgeting and eliminating up-front capital investment and unplanned costs.

- **Lower costs** – you will be utilising an existing, live, shared platform operated within a secure environment to ISO27001 standards by permanent BT staff. The provides significant economies of scale in terms of:
  - Cost savings: compare our costs with specifying and acquiring new hardware, managing commercial relationship with suppliers, designing and building the platform architecture, siting it in a secure data centre, managing it, and maintaining it 24*7*365.
  - Licence costs: your renewal price will reduce as other customers join the service.
  - Time savings: what is the lead time on your hardware supplier? This platform already exists and is being run by BT, therefore, with a little configuration, your organisation could be up and running very quickly.

- **Flexible payment mechanisms** – our charges are based on a number of simple and transparent models which can be customised to fit with your requirements:
  - per user, per annum
  - per transaction
  - capped usage

- **Exploiting BT’s track record** – BT is a renowned and trusted provider of IT services around the globe. We have a particularly successful track record in managing security systems within the finance and Critical National Infrastructure arenas.

- **Online banking fraud up 185 per cent in the first six months of 2008**

(Source: APACS, October 2008).

By offering the service from a shared platform, BT has substantially lowered the total cost of ownership of risk-based fraud reduction. There are many other benefits to be gained from partnering with BT:

- We are a well-established service provider, able to demonstrate substantial relevant track record.
- Our service is reliable and extremely secure, using a fully resilient and highly available platform with multiple layers of security.
- We manage all third parties on behalf of our customers and ensure that their contribution is similarly trustworthy.

1 One-off set up charges may also apply.
How the MFR service works

Deployment

The BT MFR service comprises a number of complementary elements which ensure a smooth route to implementation:

- An initial consultancy phase to establish your organisation’s business drivers and technical needs.
- A service configuration phase.
- Specification of easy-to-use web services calls to enable your organisation to interface your existing web applications into the BT service.
- Deployment of default rules and policies to get you started, plus training to help you add to them per your application-specific requirements.
- Collaboration on testing of the service in conjunction with your existing web-based services.
- Service support for your own end-user-facing 1st line helpdesk.

Operation

Using simple web calls, your application will supply the OAAM ‘risk engine’ with all the parameters it needs to calculate a risk-score and make a recommendation on how to handle each transaction.

For example, the risk engine will examine:

The Device ‘Fingerprint’: cookies, flash objects, device forensics, id number, etc, are all used to recognise the device on subsequent logins and determine whether or not the transaction is coming from an unknown device. The system can also check historical data to see if it is plausible that the user has physically travelled between two locations in the time available between the transactions.

The User ‘Fingerprint’: the system learns to recognise each user’s typical behaviour, including the type and value of transactions they make, the times at which they make them, etc. Deviation from the normal routine raises the risk score, but because the system learns, new behavioural patterns become accepted as normal.

Other factors considered in generating the risk score include:

- Historical data: user history, device history, location history, workflow history.
- Organisational data: e.g. billing data, shipping records, etc.
- 3rd party data: IP address intelligence, white/black listings.

These parameters are all processed in the rules and policies you define, which can be tuned and refined at your convenience to ensure the maximum amount of fraudulent transactions are blocked with minimum inconvenience to the customer.

Support

BT can also assist with:

- Provisioning second factor credentials to your end user population. Examples might be APACS-CAP smart cards and associated card readers or OATH-compliant one-time password tokens.
- Integrating your existing web applications into the BT service.
- Extended support.

- UK finance body reports that ‘Card Not Present’ retail online fraud transactions increased by over 150% in the 3 years to 2006. (Source: APACS ‘UK Payment Statistics 2007’)

CUSTOMER DOMAIN

BT DOMAIN

Risk Score

Id Verification

Strong Auth.

Options

History

BT MFR Service

SCORE, ACTION, STEP UP REQUEST

Existing or augmented logon

Optional token

Customer Online Service

Via WEB SERVICES

TRANSACTION / DEVICE DETAILS

CUSTOMER DOMAIN

BT DOMAIN
Why BT?

BT’s Managed Fraud Reduction service offers a market-leading opportunity to protect your online services from fraud and provide your end-users with confidence-boosting extra security at lower cost and with less involvement of your own personnel than would be the case in a similarly-scoped in-house development.

Security and resilience

The platform architecture is fully resilient, with mirrored processors and power supplies, and operates on a 24*7*365 basis, using:

- Physically secure server farms.
- Hardened operating systems.
- Managed firewalls (EAL4) and TLS protecting all access to the platform.
- Network-based Intrusion Detection (NBID) across all network interfaces to the platform.
- FIPS 140-2 Level 3-accredited nCipher payShield hardware security modules (HSMs) storage of cryptographic key material.

About the BT IAM portfolio

The BT Managed Fraud Reduction service is part of the BT Identity and Access Management (IAM) portfolio. BT offers a complete suite of IAM services:

- Quick Start IAM maturity assessment and diagnosis
- Consultancy on strategy options and possible routes to improving operational effectiveness
- Professional / managed service delivery of: fraud prevention services; identity credentials; registration services; authentication and authorisation services; provisioning; logical and physical access; single sign on; directory services; identity federation.

Call your BT representative for more information on any of our services.

BT partners with the major suppliers in the IAM arena offering you ‘best-of-breed’ technology at the heart of professionally managed services – designed to provide you with maximum capability for minimum disruption.

What next?

If you want to know more about how we can help your organisation then contact your BT Account Manager and arrange a meeting to discuss the Managed Fraud Reduction service in more detail.

Offices worldwide

The ICT services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc’s respective standard conditions of contract. Nothing in this publication forms any part of any contract.

©British Telecommunications plc 2008
Registered office: 81 Newgate Street, London EC1A 7AJ
Registered in England No. 1800000

Designed by TechniKa: Brighton

PHME