



Australian Government

Department of Communications,  
Information Technology and the Arts

## PREVENTING ONLINE FRAUD



# The Anomalous Behaviour Detection System



## A project to develop an anomalous behaviour detection system (ABDS) was awarded \$109 300 from round 8 of the Information Technology Online (ITOL) program.

Using state-of-the-art technology and profiling techniques, the ABDS project sought to develop a prototype to detect and reduce online banking fraud.

The project was developed by a consortium comprising three major Australian banks and Neuragenix, a Melbourne based company specialising in the development of security and compliance software. It was the first project of its kind in Australia.

## The problem of online security

Online banking is one of the most successful stories to emerge from the advent of e-business in the 1990s. It provides unprecedented flexibility for consumers while reducing processing and servicing costs for banks. However, for e-business to realise its full potential, consumers and businesses must have confidence in the security of online transactions.

Traditional shopfront banking developed a framework of security measures over many decades. In the early days of online banking, comparable controls were not in place. Banks established straight-through automated processing (STP) in the 1990s to automatically process large volumes of electronic transactions. While STP can reduce back-office processing costs and the potential for human error, it also makes it increasingly difficult to detect and contain fraudulent behaviour.

The challenge for the ABDS team was to develop a flexible, automated system to quickly and accurately identify small numbers of fraudulent transactions within large volumes of online transaction data.

## Collecting the data

To develop a system with the ability to recognise online fraud, the team first had to collect and analyse numerous fraudulent transactions. The difficulty in gathering comprehensive and coherent data sets became evident in the early stages of the ABDS project.

- Detection methods employed at the time were manual. It took anywhere between 24 hours and two weeks to identify potential fraud—much too late to prevent losses.
- Far too many transactions were being falsely identified as fraudulent (false positives). On some days the ratio of ‘suspicious’ transactions reviewed to fraudulent transactions identified was more than 1500 to 1.
- While Australian banks have been collecting transaction data and maintaining records for many years, the data did not necessarily help identify and detect emerging fraud patterns. It had to be organised into arrays that could be properly mined for each fraud type.

The ABDS team developed a generic rule set from the data held by one of the banks in the consortium. To identify the greatest number of potential fraud scenarios, the data set had to be as comprehensive as possible. The team collected data from live transactions in real-time, near-real time and overnight batch runs. More than 24 million transactions were ultimately made available to the Neuragenix team, including online transfers (75 per cent), BPAY (23 per cent) and one-time transfers (2 per cent).

They used patented technology to learn the characteristics of fraudulent transactions. The system could then use the profiles to recognise the fingerprints of subsequent cases of online banking fraud.



### **Profiling fraud**

The ABDS team then used a number of techniques to categorise the 24 million transactions and develop profiles of the known cases of fraud.

### **High-risk scenarios**

The team preconfigured and tailored scenarios to spot behaviour known to be associated with fraudulent transactions.

### **Anomalous behaviour**

They considered known online banking risks and any deviation from the normal behaviour of user and peer groups.

### **Transaction fingerprint analysis**

They used patented technology to learn the characteristics of fraudulent transactions. The system could then use the profiles to recognise the fingerprints of subsequent cases of online banking fraud.

### **Developing filters**

After the profiling techniques were applied and tested against seven million transactions, the team found they needed more complex and flexible algorithms. While terms such as phishing, spyware and keylogging are better understood today, the ABDS project was breaking new ground in 2003 as new types of fraud surfaced.

The team enriched the base data and varied the algorithms until they had profiled every instance of fraud identified in the test data. They also ensured that the parameters they set would reduce the false positive rate to an acceptable level.

Using the profiles of known fraud, the team was able to apply filters to identify and protect against the same fraudulent patterns in the future. To enable users to identify emerging fraud trends and apply new filters, they made the ABDS flexible enough to allow users to build in new detection scenarios.

# Outcomes

**The ABDS project demonstrated that an automated detection tool could significantly improve the ability of financial institutions to deal with online banking fraud. In the longer term, the project could possibly be used to address other types of financial crime.**

The solution offers the following potential benefits for banks that choose to adopt it:

## **Increased efficiency, accuracy and flexibility**

The ABDS prototype increases the speed of detection by monitoring every online transaction and automatically identifying abnormal behaviour. The system also increases the accuracy of detection by reducing the number of false positives, while its flexibility allows banks to keep pace with the emergence of new kinds of fraud.

## **Greater confidence in online banking**

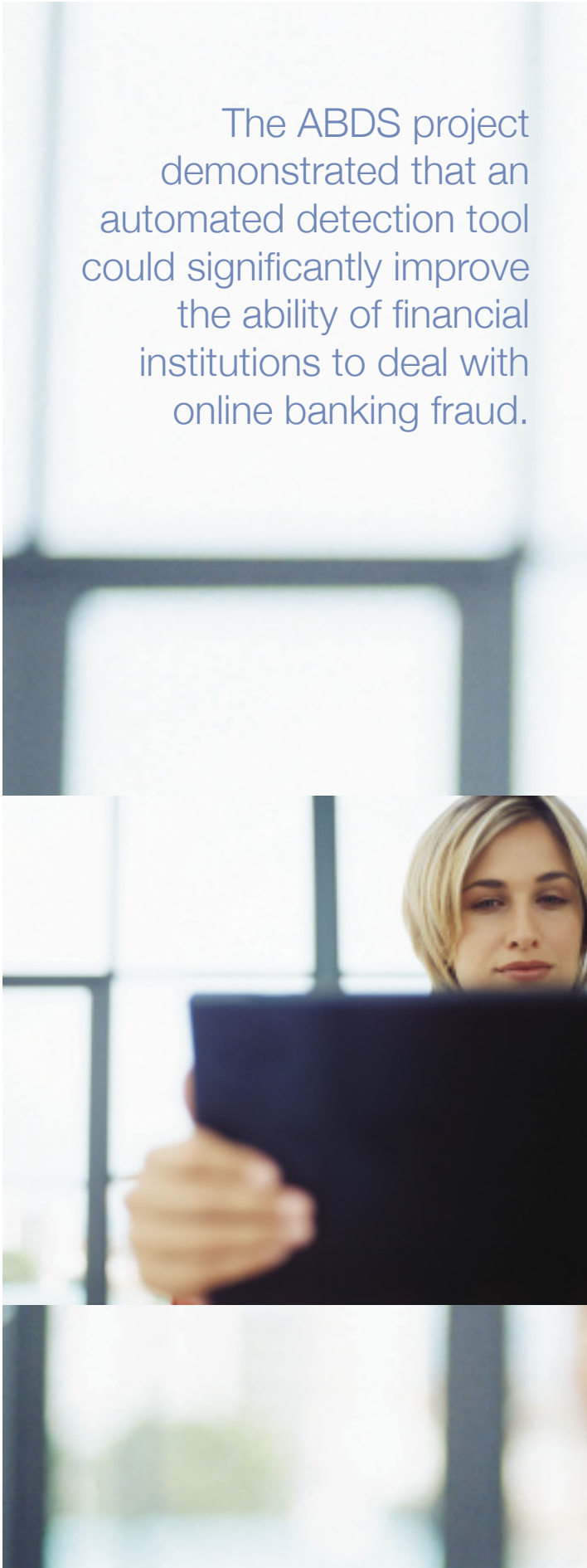
Through faster and more accurate detection, banks using the ABDS should be able to address customer complaints more quickly and activate measures to limit or even prevent online fraud. This should raise consumer and business confidence in the online payment system and in the use of the Internet as a business medium.

## **Lower costs**

By reducing the cost of fraud detection and prevention, in terms of both time and money, the ABDS should enable banks to concentrate valuable resources on finding new types of fraud.

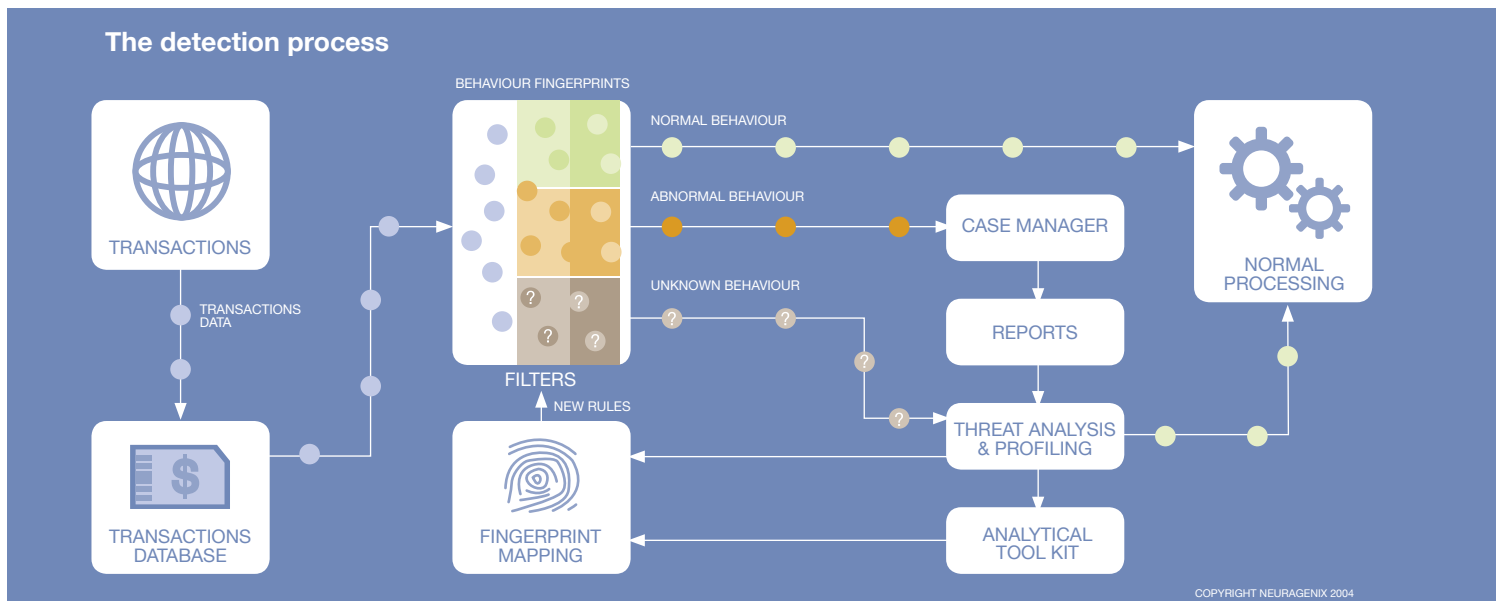
Recognising the value of the ABDS prototype, Neuragenix is integrating the system into its case management solution, Casegenix. Casegenix reports on, assesses and investigates detected irregular behaviour. This allows financial institutions to identify new fraud patterns and develop preventative measures earlier.

Neuragenix has already implemented Casegenix for two Australian banks and, in conjunction with Mantas Inc., for five Tier 1 financial institutions in the United States. Mantas is an award-winning global provider of behaviour-detection technology which joined forces with Neuragenix in December 2003. Following the success of the Casegenix arrangement, Neuragenix and Mantas are exploring new options for collaboration; options which may mean an increasing use of the ABDS solution in the future.



The ABDS project demonstrated that an automated detection tool could significantly improve the ability of financial institutions to deal with online banking fraud.

# The Future



**While the improvements to fraud detection rates have the potential to halve fraud losses in a static environment, the online banking environment is dynamic. Attack patterns are constantly changing, becoming more organised and sophisticated. The ABDS solution provides a solid foundation, but no single system can solve the issue of fraud losses.**

Like Neuragenix, organisations that deploy the ABDS will need to integrate it into a broader security strategy. This strategy should blend continually changing detection methods with customer awareness programs, improved business processes and more robust governance systems.

The Basel Committee on Banking Supervision, an advisory group on banking best practice comprising members from 10 countries, recognises these issues and has distributed governance guidelines known as the Basel II framework. In response, banks are implementing measures to ascertain the accuracy, completeness and reliability of transactions and information.

To comply with international regulations, banks may need to revisit their policies, procedures and reporting processes. Peak bodies such as the Australian Bankers Association have begun enforcing the regulations and are determining the best way for Australia to proceed.

National and international banking forums are discussing other security measures such as security seals and merchant trust marks, but these are only one step towards building trust. To gain the confidence of consumers and business, banks could also consider steps to increase awareness about online banking, limit consumer liability, and simplify avenues for the prosecution and redress of fraud.

The ABDS prototype is a definite move forward for the detection and prevention of online banking fraud. However, this is an ongoing process and improved detection is only one side of the security solution. By pursuing innovation and best practice in relation to online security, Australian financial institutions have the opportunity to enhance their standing in the global market.

DEPARTMENT OF COMMUNICATIONS, INFORMATION TECHNOLOGY AND THE ARTS  
[www.dcita.gov.au](http://www.dcita.gov.au)

### Further information

If you would like more information about Australian Government support for innovative IT projects, check our website [www.dcita.gov.au/itol](http://www.dcita.gov.au/itol)

You can email us at [itol@dcita.gov.au](mailto:itol@dcita.gov.au)



This guide has been developed by the Department of Communications, Information Technology and the Arts (DCITA) in consultation with other relevant agencies. While DCITA has made reasonable efforts to ensure that the material in this guide is accurate and up-to-date at the time of publication, DCITA cannot guarantee this. You should therefore exercise your own independent skill and judgement before you rely on the material published here, and in any important matter you should seek professional advice relevant to your own circumstances.

ISBN 0 642 753 164

© Commonwealth of Australia 2005

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth available from the Department of Communications, Information Technology and the Arts.

Requests and inquiries concerning reproduction and rights should be addressed to the:

Commonwealth Copyright Administration  
Attorney-General's Department  
Robert Garran Offices  
National Circuit  
Barton ACT 2600

or posted at [www.ag.gov.au/cca](http://www.ag.gov.au/cca)

September 2005