



National Australia Bank

Foils Fraudsters with PRM

**National Australia Bank
Melbourne, Australia**

Brett Small, Head of Consumer Banking Fraud

Brett Small seems an unlikely sting artist. As head of consumer banking fraud at the National Australia Bank, one might expect him to be straight-laced and, well, stodgy. But when he describes a recent event in which NAB foiled the brazen plans of an Internet banking fraudster—aided by Proactive Risk Manager software from ACI and a healthy dollop of in-house creative genius—the delight in his voice is palpable.

“This was a case involving a fraudulent IP address that we’d seen before,” said Small. “The customer had been targeted by the fraudster and had seen some of his savings removed from his account within a short period, but because we detected the fraud at login, we were able to contact the customer immediately and verify that the transaction was unauthorized. We then phoned the merchant that the funds had gone to and worked with the police to organize a drop-off of the 200 fraudulently purchased shoes to a local address in Melbourne. In the end, the fraudster was apprehended, and the customer didn’t lose any money. It was a fantastic result.”

FOCUS

Until a year and a half ago, Australia hadn’t seen much in the way of Internet banking fraud. This is somewhat surprising in retrospect, given the “faster payments” nature of the country’s online banking environment. Australian banks take just 12 to 24 hours to settle bank-to-bank transfers; transfers made within the bank, even between different account holders, were historically settled immediately.

That changed when fraud gangs, primarily from Eastern Europe, cast their eye on the Australian banking institutions. “Quite quickly we saw an increase in attempted fraud activity including the use of phishing emails,” recalled Small.

This spike led most Australian banks to institute a 24-hour delay for internal transactions. NAB understood that a number of approaches were required if they were going to offer their customers the best possible security and minimize losses.

“We knew that delayed payments would help but that improvements in prevention

and detection were required if we were really going to make an impact,” said Small.

“We introduced a number of measures including a robust second factor authentication service free for our customers and then turned our eye on improved detection through the use of PRM. As a result, we have cut our Internet banking losses to approximately one percent of what we were seeing at the same time last year.”

WINNING COMBINATION

The secret to NAB’s success was a combination of innovative thinking and robust PRM software. “We went live with PRM in June 2000,” said Small. “Initially we just used it for credit cards. But when Internet banking fraud started to increase slightly a few years ago, we customized the software to accept online and telephone banking transactions.

“We’ve made tweaks to the Internet banking-specific technology within PRM, allowing us to increase our

detection rate. We are now detecting almost all of our fraud.”

Small and his team started their counterattack by looking at IP addresses. (An IP, or Internet Protocol, address is a unique identifier for anyone who is connected to the Internet.) “We found strong trends around IP addresses and NAB Internet banking accounts that had been compromised,” said Small. “We wrote some reports within PRM that accessed data on fraudulent IP addresses within the PRM database. As a result of this technique, we were able to identify a significant portion of compromised accounts before funds have even been withdrawn. This has definitely helped us protect our customers.

“We then asked ourselves, ‘How do we tweak the PRM rules to make sure we can detect most if not all of those transactions on the remaining one third of accounts?’ We were confident that we could come up with a solution because PRM probably has the most flexible rules engine of any risk management tool on the market.”

“The flexibility in writing rules in PRM is virtually unparalleled. There’s no possible way that we could have made the changes we’ve made within any other product. PRM is pretty much the only tool that will allow you to do that.”

“The exciting thing for me, especially in Internet banking, has been coming up with concepts and ideas, being able to implement and customize them and seeing the uplift in detection and significant loss reduction.”

The team developed several techniques to increase detection. These techniques provided a strong profile for each customer based on their behaviors and patterns. “We built a number of tables in the PRM database to store this information in a format usable to the rules engine,” said Small. “This makes it possible to quickly identify transactions that don’t fit the customer’s normal usage profile, helping our operators make intelligent decisions when they’re working through their alerts.”

The second area of focus was the relationship between customers and the origin of their transactions. “Most customers login from home and work, so they have a very distinct footprint,” said Small. “The specifics of their footprint may change from time to time, but for the most part it remains similar. Using PRM, we are able to establish an expected footprint for our customers and therefore identify which Internet banking logins and transactions to treat as potentially suspicious.”

Using these two simple techniques, PRM eliminates around 98 percent of all transactions before the rules are even applied. “We’re able to remove the lion’s share of transactions from alerting in the system,” said Small. “From that point forward, our customized PRM rules scrutinize every transaction that doesn’t meet those two criteria. This allows us to pick up virtually all Internet banking fraud.”

KEY FEATURES

For Small, a number of key features set PRM well apart from competitive offerings. “I’ll go back to the rules engine,” he said. “The flexibility in writing rules in PRM is virtually unparalleled. There’s no possible way that we could have made the changes we’ve made within any other product. PRM is pretty much the only tool that will allow you to do that.”

PRM’s graphical user interface also wins praise. “It’s very intuitive,” continued Small. “A lot of Internet banking tools out there don’t have that level of maturity in the detection area. They might do some fancy things behind the scenes, but the actual tool that’s presented to the operator is not particularly flexible.”

NAB is not an institution that rests on its laurels. Moving forward, the bank expects to move closer to 100 percent detection through the use of “aggregates,” a technology within PRM that will enable a smarter solution with more in-depth rules around fraud. Another exciting project based on PRM will tackle the growing problem of identity theft. Also contemplated is the introduction of ACI Automated Case Management software into NAB’s fraud control environment. “We handle multiple fraud areas within the same team, and we’ve been looking for a case management solution that

everyone can use,” said Small. “ACM appears to be a very good answer. The intuitive workflow capability of the product will allow us to increase our rigor and processes to an even greater level and also automate the small percentage of our work that is still paper-based.”

PRM creates an environment in which creative ideas can flourish. “The exciting thing for me, especially in Internet banking, has been coming up with concepts and ideas, being able to implement and customize them and seeing the uplift in detection and significant loss reduction,” said Small. “Literally as soon as we’ve put each of these steps in place with PRM, we have seen instant and dramatic declines in fraud-related losses – which helps us and our customers.”

PRM creates a solid foundation for NAB’s innovative approach to combating Internet banking fraud. “Most tools I’ve seen—especially around Internet banking, but also in other areas—have very closed rules engines,” concluded Small. “I would say that PRM probably stands alone in the power and flexibility of its rules engine. In my opinion, that’s the main reason we’ve been able to achieve such effective fraud mitigation at NAB.” ▲