



Intelligent Security: Countering Sophisticated Fraud

The sophistication and increasingly widespread availability of advanced fraudulent techniques such as Man-in-the-Middle and Man-in-the-Browser has forced a re-think on how Banks and other organisations combat electronic fraud. Intelligent security solutions provide the opportunity to not only counter fraud and increase customer confidence, but to also fully exploit the Internet channel for Business Enablement whilst providing new intelligence to support risk and compliance strategies.

Customer Authentication – No Longer a Sufficient Means of Protection

A number of seminal fraudulent incidents during 2006 and early 2007 have raised the awareness of electronic fraud from the backroom to the boardroom, whilst also signalling a shift in electronic security strategy, in terms of both a holistic, multi-channel approach and a re-evaluation of what Customer Authentication actually provides.

The real impact of Man-in-the-Middle (MitM) and Man-in-the-Browser (MitB) has been the realisation that Customer Authentication, including Strong (multi-factor) Authentication, whilst being sufficient for certain transactions, by itself cannot prevent MitM and MitB attacks. These attacks have necessitated the requirement for Out-of-Band (OOB) Transaction Verification *in addition* to Strong Authentication.

At ValidSoft we believe that the most effective way to protect all bank customers from sophisticated fraud, including MitM, MitB and Trojans is to add a fully automated "out-of-band" capability. This enables the customer to verify the transaction details, in real-time, via a phone call that replays the transaction received by the bank so that the customer can confirm that transaction integrity has been preserved.

Out-of-Band Transaction Verification verifies the integrity of the transaction itself, alerting the customer to any corruption or tampering of the genuine transaction content, or even the creation of additional fraudulent transactions, thereby preventing the customer from unwittingly authorising such transactions.

Out-of-Band Transaction Verification coupled with Strong OOB Authentication provides not only a highly secure authentication solution, but also a tool to automate manual fraud processes and migrate manual business processes onto the cost-effective Internet channel.

Automating the Resolution Process of Transaction Anomaly Detection (TAD)

Potentially fraudulent transactions, identified and intercepted by TAD or Risk engines, require resolution of the potential anomaly. Typically, anomaly resolution is performed manually after the event. This involves an employee of the Bank, or Call Centre, contacting the customer by telephone in order to ascertain whether they did indeed perform the on-line transaction in question. This process is costly, unreliable insofar as actually making contact with the customer and insecure as it involves a manual telephone call that reveals security credentials to unknown third parties.

As electronic banking channels increasingly move to real-time transaction processing, the timeframe for dealing with anomalous transactions must also occur in real-time, i.e. before the transaction is committed. The introduction of Faster Payments in the UK in late 2007 is a case in point.

However, by automating the anomaly resolution process, and performing it in real-time, Banks can overcome all of the present issues associated with manual follow-up whilst also complying with real-time payments Initiatives, in a secure, timely and cost-effective manner. To securely automate this process requires Transaction Verification in addition to Strong Authentication, as it will increasingly be the transaction content that triggers the anomaly.

Consumer Confidence – The Market Opportunities

It is estimated that in Europe, almost 50% of Internet users, or 80 million people, don't bank online, with security fears being one of the biggest barriers to online banking adoption. Of this number, almost 10% have given up on online banking. A similar situation exists in the UK representing almost 15 million Internet users that don't bank online. Almost 50% of these users are concerned about security which represents a significant opportunity for those banks that can address the security concerns of this large potential customer base.

In addition, as the internal cost to a bank of an Internet based transaction is a fraction of the cost of a branch or phone banking transaction, these figures represent a significant hidden administrative cost to the banks and have a direct adverse affect on Cost Ratios.

These figures, however, are predicated on the fraudulent techniques we have seen to date and the current perception of Internet banking security. The sophisticated fraud now in evidence has the potential to further erode this consumer confidence. A combination of negative press, potential litigation and a perceived inability of institutions to offer a viable or convincing solution could see an escalation in the defection away from Internet banking.

For those banks that seize the initiative in terms of offering truly secure Internet banking, there is also a clear opportunity, not just in reducing transactional costs within their existing customer base, but also in attracting new customers who are not offered similar secure services with their present institution. These figures indicate a sizeable latent demand for secure Internet banking and a reason why security will be viewed as a significant marketing differentiator between institutions.

Leveraging Strong Security for Business Enablement

Combining Strong Authentication with Transaction Verification provides the security necessary to ensure the integrity of a transaction and the identity of the user. This, in effect, creates a Business Enabling technology that allows organisations to exploit the cost-effective Internet channel by allowing their customers to perform more self-service functions.

Transactions that traditionally have not been considered suitable for online processing, such as customer or account maintenance processes, e.g. Change of Address forms or loan applications, that carry a high risk, can now be considered for migration to the Internet channel. Not only will the security afforded create a more consistent, accurate, timely and secure process than the corresponding manual practices in place today, but it also empowers customers and creates potentially significant cost savings for the institution.

Viewing this technology as a Business Enabler and differentiating on it will allow those financial institutions to gain even more leverage out of their investment in both the Internet channel and the tools employed to secure it.

Leveraging Intelligent Security – Predict; Prescribe; Pre-empt

Using real-time, connected Authentication models through telephony offers banks intelligent options not available through static, disconnected devices.

Our Risk Adjusted Rules Engine (RARE) enables dynamic rules (triggers) to be applied to any transaction in real-time, forcing an authentication/verification when invoked. Technologies such as Transaction Recording and Biometric Voice Verification for Non-Repudiation, and Operator Breakout for potentially fraudulent transactions can all be combined in a seamless and invisible way to provide a new direction in Risk and Compliance strategy, combining Prediction of threat, Prescription of countermeasure and Pre-emption of attack. Yet, the experience from the customers' perspective is consistent and remains simple, intuitive and easy to use.

Find out more

If you would like more information contact: