# Winning the Battle Against Internet Banking Fraud by Leveraging Real-Time Data Integration


Keith Evans >> Shadowbase Product Management >> Gravic, Inc.

Who among us has never received an email purporting to come from a bank or other financial institution, stating that due to "suspicious activity" or some such subterfuge, our account has been frozen until we click the URL in the message to "reset" our account? Of course, this will require divulging personal information such as our user ID, password, home address, etc. That information is then used by crooks to steal money or obtain further personal information, such as account numbers. This, of course, is an example of phishing, and it is a very lucrative enterprise too. In the UK alone, internet banking fraud in the first six months of 2014 cost £29.3M.[1] Globally, the cost is measured in the tens of billions of dollars annually. Email phishing is just one avenue; phone calls purporting to be from agents of your bank and computer viruses are other ways this information is obtained. Simply buying it is also an option. Cybersecurity firm Hold Security revealed recently that it discovered stolen credentials from some 360 million accounts available for sale on the underground internet.

With the information necessary to access online bank accounts so readily available, how is a bank to defend itself (and us) against this ever increasing threat? And not just to defeat the fraud itself, but do so in such a way that enables prosecution and conviction of the perpetrators so they cannot just do it again? This article describes how this goal has been successfully achieved by a major European retail bank.

## One Bank's Internet Banking Fraud Detection System

In the bank's home country, the laws regarding fraud and what constitutes a crime are very specific. Stealing a user ID and password, and then using that information to log in to a customer's internet banking account, while exhibiting an intent to commit fraud, is not necessarily criminal in and of itself. It is necessary that an actual act of fraud be perpetrated, such as transferring money from the customer's account to another account.

This fact necessitated the bank to design and implement its internet banking application in a very specific way: to detect and prevent fraud, yet still enable the authorities to pursue a conviction against the actual actions committed. For example, simply denying a suspicious logon, while protecting the bank, would not provide sufficient grounds for prosecution.

The basic structure of the bank's internet banking and real-time fraud detection system is shown in Figure 1. The internet banking application runs on HP NonStop servers. Changes made by that application to the banking database (primarily implemented using HP NonStop SQL), are read from the HP NonStop TMF audit trail by the Shadowbase® data replication product from Gravic, Inc.[2]

The changes are fed by the Shadowbase replication engine from the HP NonStop server via a TCP/IP connection to Shadowbase processes running on a Linux system. From there, customized user exit procedures running inside the Shadowbase processes structure the changes into an architected message format (similar to a CSV file), and feed those messages via TCP/IP into a RiskShield® fraud detection application.[3] To facilitate low latency yet improve overall efficiency, the changes are batch fed 50 at a time into RiskShield, or whenever a timer expires if 50 changes are not received within that timeframe.

The RiskShield application contains a knowledgebase which allows it to detect and flag potentially fraudulent transactions (for example, User IDs whose credentials are known to have been compromised, known target accounts for fraudulent money transfers, etc.). Having analyzed the input messages (customer ID, source account, target account, amount, etc.), the RiskShield application returns a response to the internet banking application via a private connection, indicating whether or not the transaction is suspicious. The internet banking application then proceeds accordingly.

What is very clever about this system is the way in which it is architected to serve both the needs of the bank in preventing fraudulent transactions from completing, and in allowing the online activities of the criminals to proceed, to the point where an actual act of fraud is committed, for which they can then be prosecuted. To accomplish this, the system splits the internet banking business activity into a series of steps (Figure 1), with each step comprising a separate TMF transaction, up to a final step which will complete the business activity.

For example, when a criminal intends to transfer money from another account to their own account, the first step is the user authentication process. The user ID and password information are captured by the internet banking application and are logged

[1] Source: Financial Fraud Action UK.
[2] For more information, please visit www.gravic.com/shadowbase.
[3] For more information, visit www.inform-software.com/products/riskshield.

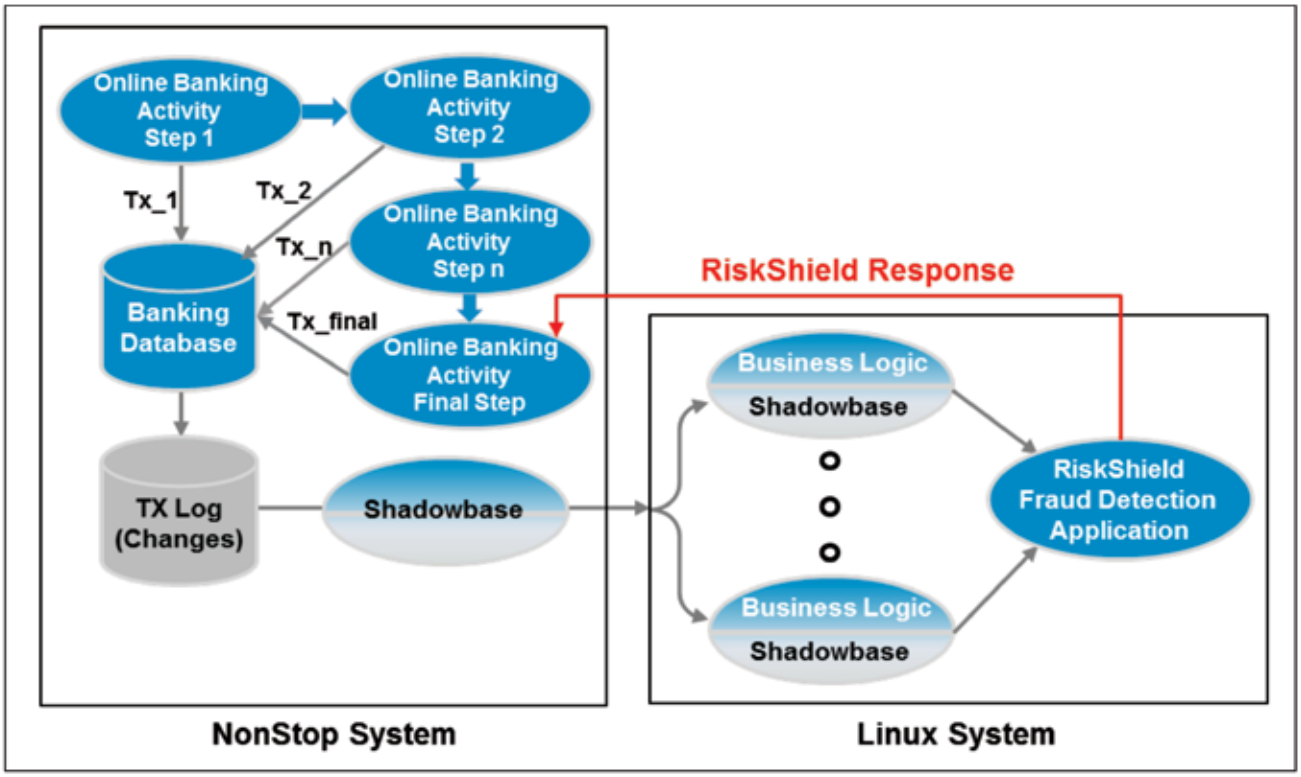


Figure 1 – Internet Banking Fraud Detection System

in the banking database via a TMF transaction. This information is read by Shadowbase replication from the TMF audit trail and via the process described above would quickly be delivered to the RiskShield application, which could then begin its analysis. Even if an immediate response was returned by the RiskShield application flagging the transaction as suspicious, the bank would allow the activity to proceed, since an actual criminal act has not yet been committed. Meanwhile, the next step of the internet banking activity proceeds, which might be to validate whether there are sufficient funds in the source account to satisfy the transfer. Likewise this transaction would be logged and delivered to the RiskShield application. For some accounts, rules may have been established which limit the amount of transfers, especially if they are destined for overseas accounts.

The RiskShield application includes this additional information with that already received and continues its analysis. The next step for the internet banking application is to validate the target account for the transfer. Again, the banking database is updated with this information, which is forwarded by Shadowbase technology in real-time to the RiskShield application, which adds yet another piece of information to the puzzle.

Finally, the criminal is presented with a confirmation screen by the internet banking application, showing the FROM and TO account information, the amount to be transferred, and is asked if the information is correct to click an "Execute Transfer" button. When that is done, the final phase of the business activity and the final TMF transaction is started by the internet banking application. If by this time a response has been received from the RiskShield application indicating that the activity is suspicious, the final TMF transaction will be aborted, the money transfer is not performed, and the fraud is prevented.

The bank will then take further steps as appropriate, for example, notifying the actual account holder that their credentials have been compromised, and suspending the account (just like the phishing example above!). But most importantly, because the criminal activity was allowed to proceed to the point where an actual crime was committed (the attempt to fraudulently transfer money from one account to another in this example), the bank will contact the authorities and provide them with all of the details captured by the internet banking and RiskShield applications, enabling them to pursue an investigation and possible criminal prosecution.

There is a very interesting point to note with the operation of this fraud detection system. If the response from the RiskShield application is not received by the internet banking application by the time of the final step in the activity (by the time the "Execute Transfer" button is clicked in our example), the bank may nevertheless complete the activity (perform the transfer in this case). If subsequently the RiskShield response indicates possible fraud, the bank will then take the necessary steps retroactively. While not ideal from the fraud prevention perspective, this approach can be taken because the bank does not necessarily want to delay a user transaction every time the fraud response is unacceptably "slow" in order to catch the few (by comparison) fraudulent activities. The internet banking application is optimized for the normal, non-fraudulent case, with reasonable time limits for response time. This approach illustrates the tension between the bank's need to prevent fraud, while not negatively affecting normal business or customer service.

Another interesting facet of this application is that there are aspects of big data analytics, application integration, and real-time business intelligence (RTBI) involved.[4] There can be as

[4] For more information, please see these white papers: Shadowbase Solutions in a Big Data World, Shadowbase Streams for Application Integration, and The Evolution of Real-Time Business Intelligence and How to Achieve it Using Shadowbase.

many as 5,000-6,000 transactions per second moving through this system, which requires the reading and distribution of a very large amount of data by Shadowbase replication, between heterogeneous applications (running on HP NonStop and Linux systems), as well as analysis of this data by the RiskShield application – all in real-time and with the addition of minimal latency and overhead.

## Conclusion

Fortunately, the system is working! Figure 2 shows the cost of internet banking fraud in the bank's home country over the past few years. While it had been increasing exponentially until 2011, since then – due to the implementation by banks of more and more sophisticated fraud prevention schemes, such as the one described here – the cost of internet banking fraud in this country has declined significantly, dropping by 72% between 2012 and 2013.

This example provides a powerful demonstration of what can be achieved by clever application design, coupled with a Shadowbase high-speed/high-throughput heterogeneous data distribution fabric, to deliver large amounts of data in real-time to a data analytics engine. The result is a system which provides critical functionality and produces tangible positive results for the business. In this case the application is used to prevent internet banking fraud, and has resulted in a significant decrease in the cost of such fraud to the bank, and prosecution of the perpetrators. There are of course many other applications of such technologies to enable businesses, not only to detect and defeat criminal activity, but also to gain other competitive advantages in other markets and industries.

[5] Source: NVB, 2013.

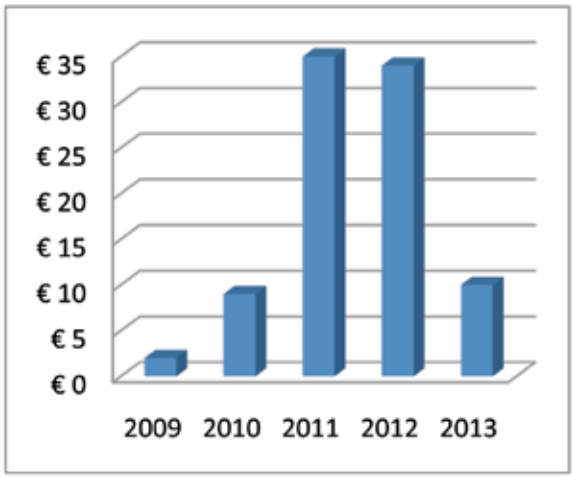


Figure 2 – Cost of Internet Banking Fraud in Bank's Home Country (€M)[5]

## The Shadowbase Data Replication Product Suite

The Shadowbase solution suite comprises several products addressing business continuity, data replication, data and application integration, zero downtime migration, and other utilities to deliver a true 24x7 "nonstop" enterprise. Shadowbase Streams change data capture technology allows companies to build real-time business intelligence systems to immediately analyze and process events as they occur in their organization, using an efficient event-driven architecture (EDA). As shown in this article, it allows disparate applications to interoperate in real-time at the data level, avoiding the need for expensive programming and middleware adapters. Shadowbase sales and support is now directly available from your HP NonStop account team, or contact Gravic, Inc. for more information.

*Keith B. Evans works on Shadowbase business development and product management for Shadowbase synchronous replication products, a significant and unique differentiating technology. Asynchronous data replication suffers from certain limitations such as data loss when outages occur, and data collisions in an active/active architecture. Synchronous replication removes these limitations, resulting in zero data loss when outages occur, and no possibility of data collisions in an active/active environment. Shadowbase synchronous replication can therefore be used for the most demanding of mission-critical applications, where the costs associated with any amount of downtime or lost data cannot be tolerated.*