HONG LEONG BANK INTRODUCES INTELLIGENT ANTI-FRAUD SERVICES FOR ITS CUSTOMERS WITH RSA

AT-A-GLANCE

Challenges

- Hong Leong Bank prides itself on the quality and security of its digital banking services. It needs to maintain its reputation by implementing cutting-edge solutions
- Its anti-fraud platform was static and unable to respond to individual customer requirements, so the bank needed a more intelligent approach

Results

- RSA FraudAction Service provides proven web fraud detection and threat management to meet the bank's standards and compliance obligations
- The RSA Risk Engine responds to individual user patterns and learns behaviors over time to offer a more personalized authentication service for digital banking customers

> "RSA Adaptive Authentication was able to individually profile each of our users' behavior and to actually continuously learn their new behaviors. We were convinced that the system was able to achieve a high rate of detection and minimize the rate of false positives."

EDWARD LAM, HEAD OF REGULATORY COMPLIANCE, SECURITY MANAGEMENT AND SELF-SERVICE TERMINAL DEVELOPMENT

HongLeong Bank

RSA

Hong Leong Bank is a public listed company based in Malaysia. It is a part of the larger Hong Leong Group, which has operated in the financial services industry since 1968.

How mission critical is security to your business?

From a digital banking perspective, security is paramount for us. Together with risk management and regulatory compliance, it is a key consideration in everything we do. We need to keep in mind that for whatever products and services we offer, we have to make sure that the customer is able to transact it conveniently and securely on our platform.

Digital banking is one of our strategic pillars, and we need to ensure that we're offering the best digital solutions and e-payment capabilities to our customers. Of course, customers are going to be concerned about the security of their bank account – they need to know that they're banking safely. If we don't adopt the latest in security innovation, then our customers will lose confidence in banking with us, and our business would suffer.

What is the main security priority within your business?

Our main focus is fraud detection. We deploy specialist knowledge and key technologies to detect and prevent a fraud incident, and if we catch an attack in progress then we can contain it. However, it's not just down to our team of developers, IT teams and our fraud management unit. We also need to ensure that our customers are aware of the risks and consequences of fraud. Security is a joint responsibility between the bank and the customer, and customer education plays an important role.

What security challenge were you looking to address with RSA?

Before we implemented the fraud detection system we were practicing static security - we used a system that imposed the same security measures regardless of a customer's usage behavior or service profile. Unfortunately, it's akin to adding more locks to the same door. We couldn't rely on conventional security measures, and we needed to ensure that we could quickly adapt to new threat behavior in the field.

In terms of what we needed from a security solution, we had to make sure that it worked with our existing resources. This meant that our teams of fraud analysts and IT staff needed to make the best use of any technology and provide the human intelligence needed to make the best decisions.

Why did you choose to work with RSA?

What we liked about RSA was the clarity of the solution it presented to us. It offered a risk engine which was able to individually profile each of our users' behavior and to continuously learn their new behaviors. We were convinced that the system was able to achieve a high rate of detection and minimize the rate of false positives. On top of that, we also deployed RSA FraudAction services to address threats external to the bank.

Can you provide an example of how RSA helped your business fight fraud?

In Malaysia, the two main types of scam we face are phishing and phone scams. For phone scams it's basically identity theft, where the fraudsters are trying to secure the necessary credentials for them to register for banking. For example, we caught wind of a very particular scheme where the customer received a phone call from a fraudster, and was persuaded to change the phone number associated with his bank account to that of the fraudster. Once he did so, the fraudster contacted the bank to request a one-time password (OTP) for accessing the account, and would receive the information over text message.

However, we detected a change in the customer's mobile number and sent this information over to AAOP. Using this intelligence, we deduced that the action was potentially associated with fraud, and we were able to detect and block the fraudster's login activity. The incident was recorded in our case management system, and the customer was contacted to authenticate the action. As a result, we actively prevented a case of fraud.

Where or how is the solution benefitting you and your customers?

We focus on three main indicators, the first being the number of disputes reported by customers versus the actual detection rate by our fraud system. We also track the volume of cases created against our resources that processed them, and the third indicator is the actual customer experience, as reported by our customers.

With the fraud detection system and the policy rules we've written, we are able to detect fraudulent activity and in some instances we are able to deter attackers from logging onto the system itself. In addition, because the system can 'learn' more about the trends it's seeing in the system and can adapt to suit its findings, we've also reduced the number of false positive results – this means that our customers aren't panicking over a false alarm, and it also means that we can deploy a small team to run the fraud detection system 24/7.

What best practices would you recommend to businesses wanting to deploy a new anti-fraud solution?

Ensure that you have a clear objective in mind before you reach the implementation stage, and know what you need before you begin the decision-making process. We took the time to research what we needed to implement the best solution, and divided it into a three-phase approach.

Firstly, we had to secure the front door. For us, this is login protection – ensuring that we can deter fraud at the login phases. It sounds like the most basic part of security, but if we can stop the fraudsters from ever getting into the account, it'll increase customer confidence.

For our second phase, we needed to gain the insight and overview of the wider landscape. This meant that we needed to collect customer data over a period of a few months; this backend task was so that the solution had an initial bank of information to refer to upon launch. That way, the security system could refer to real customer profiles when deciding whether an action is valid or authentic.

The final phase was the most complex of the three – preparing for the initial launch. Before we could switch the new system on, we needed to ensure that it had the right risk policies and procedures to hand in order to follow the chain and generate its leads. For this, we worked closely with our analysts, making best use of their years of experience to develop the rules and policies needed to run an automated system.

What's the next step in your security journey?

Last year we went live with biometric authentication, which allows our customers to perform peer-to-peer payments, cardless withdrawals, and even view bank accounts and perform retail merchant payments just by presenting their fingerprint to authenticate. In phase two we are extending the biometric authentication capability to complement our transaction signing project.

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.rsa.com

©2016 EMC Corporation. All rights reserved. EMC, RSA, the RSA logo and Security Analytics are the property of EMC Corporation in the United States and/or other countries. All other trademarks referenced are the property of their respective owners. Hong Leong Bank Berhad.