CUSTOMER Q&A

LANDSBANKINN DETECTS MORE FRAUD, GROWS ONLINE BANKING WITH THE RSA FRAUD AND RISK INTELLIGENCE PORTFOLIO

AT-A-GLANCE

Challenges

- Landsbankinn wanted to improve its customers' experience of online banking to ensure the highest levels of security and minimize the impact of fraud.
- It needed a fast and reliable solution to avoid frustrating users with long loading times.

Results

- Landsbankinn leverages RSA Adaptive Authentication, RSA Web Threat Detection and RSA FraudAction Services to gain a more comprehensive picture of who was using their online banking site and how they were using it. This allowed them to grow their online banking users and simultaneously detect more fraud.
- As a result, Landsbankinn was able to tweak its services based on customer preferences, increasing its market share by over ten percentage points and improving its relationship with its customers.
- The bank also saw an increase of around 20 percent in its customer base, and a 60 percent jump in the number of customers using its mobile banking solution.

"We started by building our customer rules in RSA Web Threat detection, using IP feeds from the eFraudNetwork and other sponsors and vendors to pull everything together in a single location. It means that we've got a better understanding of customer behaviors, the global network, attackers and users, and can deploy analytics in each area to increase our awareness of what's going on out there"

GUDMUNDUR INGVARSSON, CYBER SECURITY OFFICER, LANDSBANKINN

RSA

Landsbankinn is a leading Icelandic financial institution, working with both corporate and retail customers. Owned by the National Treasury of Iceland and serving over 40 percent of the country's population, Landsbankinn offers a full range of financial services and is considered a leader in Europe.

Why is security critical to your business?

Hákon Åkerlund, IT Security Manager: Security is a key aspect of banking so it's important to put it at the very top of the agenda. If you look at online banking, for example, customers can now bank whenever and wherever they want. This mobility poses new challenges to both banks and their security teams, who need to manage threats and customers at every endpoint. If the customer doesn't feel that their bank has the right measures, then they won't stay with them and will move elsewhere. As security professionals, our job is to make the customer experience better and assure them that their information and assets are safe.

What were the drivers behind your decision to improve your security systems?

Our main driver is customer security. We want to ensure that a customer can log onto their online account and feel safe no matter where they are, and the key to doing this is through collaboration. Joining up the dots between departments in the bank creates a cohesive strategy which in turn reassures the customer, and we're aiming to include every department in developing the best security strategy.

To do this, we needed a solution that would centralize our data on customers, so we could then examine the data to determine suspicious activity. Customers don't want to wait for their log-in portal to load while it's checking their credentials, so we needed a fast and reliable solution.

What particular challenges are you facing with online banking?

In 1998, we offered customers the opportunity to log in to their online bank account with a username and password through HTML. Even though that worked, a few years later we moved to two-factor authentication and in 2004, we implemented RSA SecurID. Throughout our experiences with online banking, we've learned that as the avenues for access change, so do the hackers – just changing a log-in system won't stop attacks for long.

Gudmundur Ingvarsson, Cyber Security Officer: Usernames and passwords can be dangerous because the majority of users are predictable – cyber criminals rely on expected behaviors to gain access to accounts. In fact, the majority of people will give up their passwords when asked, and there are always fraud cases around family matters such as divorce. As a result, we need to be sure that we have the right systems in place to protect customers and keep their information safe.

Why did you decide to deploy RSA Adaptive Authentication?

Ingvarsson: We used an advisory service within Iceland, which matches clients with providers based on their particular requirements. RSA was able to bridge our portfolio perfectly so we deployed RSA Adaptive Authentication in 2012. We've since adopted RSA Web Threat Detection and we've joined the RSA eFraudNetwork as well.

Åkerlund: We knew with our work from RSA that the company knows how to handle security at every level. Working with a reliable partner means that we can go to them with questions, problems or ideas, and they can work to support us at each point in our security journey.

What immediate effects did you see on your system following deployment?

Ingvarsson: We started by building our customer rules in RSA Web Threat Detection, using IP feeds from the eFraudNetwork and other sponsors and vendors to pull everything together into a single location. It means that we've got a better understanding of customer behaviors, the global network, attackers and users, and can deploy analytics in each area to increase our awareness of what's going on out there.

When we first deployed RSA solutions we had around 85,000 online retail banking users, and now we're closing 105,000. Overall, we've seen an increase of around 20 percent in our customer base. The actual usage rate has shot up by 40 percent in just two years, and we've also seen a 60 percent increase in the number of people using our mobile banking solution.

Åkerlund: RSA told us that right from the start that we'd see more users turning to online banking, and we can now see how they're accessing our portal. We're seeing higher page views and seeing what transactions they're making through the online portal. We've also used customer feedback to refine the portal further, and as a result we've seen our market share jump from 32 to 42 percent.

How have RSA solutions benefitted your business?

Åkerlund: Everything we do with RSA is on our terms – we're not tied into a single system, and we can tailor the solution to our needs as a business. For example, we're able to build custom rule sets which interact with customers when they try to access their bank account. If they're in an unusual location, we can then offer a further authentication check to determine whether it's really them. It also means that we can prioritize creating the right experience for our customers and make them feel as though they're protected when they use our online banking service.

Ingvarsson: With RSA solutions and the RSA eFraudNetwork integrated into the same system, it's easier to prevent fraud, by looking at all of the information available. For example, we're able to step up authentication procedures for users that come from compromised IPs and open public networks, and doing so means that we're preventing fraud cases before they happen. After implementing RSA Web Threat Detection, we can draw from other sponsors and vendors, from the open threat community, and from the emerging threats community. As a result, we've got a much better awareness of what's going on in the threat landscape and can use this information to better protect our customers.

What best practices would you share with others wanting to implement a new solution?

Åkerlund: Informing the customer about upcoming changes to their banking system is essential. We need to communicate it clearly across demographics and tailor our messaging to their specific needs. For example, elderly customers who use online banking because they can't leave the house due to illness differ from younger users who want the convenience of banking wherever they are. With that in mind, using different messaging and explanations depending on our audience worked because they then knew what we were doing and they had the full information they needed to opt into our initiative.

Businesses should also prepare their support staff for the change – after all, they'll be the ones fielding calls from confused customers. We needed to ensure that staff could confidently talk about the new system and reassure customers that their data was protected and safe. As a result, they feel prepared to handle any questions thrown at them.

What are the future plans for security at Landsbankinn?

Ingvarsson: The next step is integration between our RSA products: Adaptive Authentication, Web Threat Detection, and the eFraudNetwork. All of RSA's solutions work together as well so we can connect our RSA SecurID with our RSA Adaptive Authentication, and can then connect those to the eFraudNetwork.

We want to introduce more biometrics into our online banking systems as well. Ideally, we'd go directly to biometrics rather than transitioning from SMS and phone confirmation.

Åkerlund: We're looking to work closely with our customers to make the system convenient for them. User convenience is really important when it comes to banking. Young people just want to use their phones to do their online banking and we need to make sure that we provide them a good authentication solution within that.

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