Case study
Swift Payment Controls

Client
Khan Bank

KHAN BANK

Payment Controls: A ‘success story’ for Khan Bank

Khan Bank is the largest commercial bank in Mongolia. They provide comprehensive banking services to an estimated 78% of all Mongolian households. A trusted banking partner to roughly 2.7 million customers domestically, Khan Bank was among the first banks to introduce digital banking products and services to the country’s market. Today, 98% of its transactions are made via digital channels.

Khan Bank leverages relationships with global correspondent banks to support international trading relationships between Mongolia and South Korea, China, Japan, Singapore, Canada, and Germany. Its outbound Swift payments traffic has increased by 57 % in the last year, and approximately 70% of outgoing payments are USD denominated.

Currently, the operations department comprises of two teams. The first team oversees payments before they are processed, with 10 members of staff relying on manual controls to handle up to 1,000 Swift messages a day. The second team undertakes daily controls, reporting and monitoring activities related to processed payments and settlements.

Khan Bank is continuously improving their payment operation systems and controls. The operational improvements team is responsible for achieving this objective, by leveraging new technologies and implementing Swift solutions in the local market. They have successfully adopted Swift gpi and Transaction Screening services for sanctions compliance, and are on track to deliver their ISO 20022 programme in November 2022.

"The onboarding project management plan was clear from the start - well organised by the assigned consultant with simple steps that meant it was implemented much faster than other system development project plans. The solution has also guided and helped us to apply additional controls to complement existing measures"

Battulga M
Project manager in charge, officer of Process Improvement Department from Khan Bank side.

Challenge

To further protect their institution and community, Khan Bank sought to enhance cybersecurity and fraud prevention practices by:

- Strengthening controls against cyberattacks and fraud targeting financial institutions, as recommended within the Swift customer security control framework (CSCF). CSCF recommends a set of advisory and mandatory controls to protect the community from various risks. While the bank had already implemented primary controls in place, it continually seeks to adopt best practices by adopting secondary layers of protection.
- Addressing the rising challenge of end-customer fraud: While the bank has already implemented primary controls in their digital payment channels to detect and prevent unauthorised fraud cases, the numbers of authorised payment fraud cases has remained high. For example, the number of scams and phishing reported cases by the customers on international payments has continued to rise. This poses a problem for banks globally, including Khan Bank as they value customer experience, and attempted recall and recovery operations to retrieve funds for their customers are time-consuming and not always possible.

Onboarding Journey

Khan Bank's operational improvements team identified Swift Payment Controls as a solution to help them address some of these challenges. They became the first commercial bank in Mongolia to implement the solution.
The full onboarding project, from procurement to implementation, took just three months. Khan Bank's onboarding experience has been smooth thanks to a streamlined project plan and extensive support received from Swift. The ability to configure rules in a test environment allowed them to simulate the impact of using PCS on their messaging flows, and to refine their configuration to avoid a high number of false positive alerts before using the live environment.

"The onboarding project management plan was clear from the start - well organised by the assigned consultant with simple steps that meant it was implemented much faster than other system development project plans. The solution has also guided and helped us to apply additional controls to complement existing measures" – Battulga M., Project Manager & Officer of Process Improvement Department, Khan Bank.

Solution

Khan Bank has leveraged the full spectrum of rules offered by the Payment Controls tool, enabling them to implement a wide range of controls that are flexible to their business needs and payment activities.

To help address the need to strengthen controls against cyberattacks and fraud targeting financial institutions, the operations team analysed data from historical fraud cases. In addition, identifying and defining the regular boundaries of their business allowed them to configure rules to alert and/or block messages outside of those regular patterns, which could indicate a cyberattack or fraud attempt. They implemented a number of rules offered by Payment Controls, which they configured to trigger alerts in the following ways:

- Message Count: When the number of messages sent within a specific time frame exceeds their normal thresholds.
- Amount Aggregation: Once the aggregated value of payments has exceeded a given amount within a defined period of time. These thresholds are based on data from historical fraudulent transaction cases which have been published in the Swift ISAC portal.
- Single Payment: For a transaction sent to specific countries with known fraud - attempt cases and considered as high risk.
- New Scenario: If there is a transaction sent to a new beneficiary bank or intermediary bank i.e. cases in which payment routing has been changed.
- Business Calendar: When a payment is sent outside regular business hours, including public holidays.
- Rules Combination: To combine the risk scoring function with other rules. This provides additional insights on possible fraud incidents.

“Payment Controls also enables us to attest to the requirements within the Customer Security Programme, which mandates the implementation of transaction business controls. This will help to continue building trusted relationships with foreign correspondent banks”

Nomulin B
Team Lead of Transaction Banking Section, Process Improvement Department

When evaluating ways to prevent **end-customer fraud** by detecting such cases, Khan Bank identified and implemented a number of controls offered by the Payment Controls tool. This included the Account Monitoring rule: by regularly updating their ‘forbid’ list with account numbers of known fraudsters, Khan Bank can ensure that payments sent to those beneficiary accounts are blocked before being released. In turn, this offers time for them to investigate those payments with the customer or counterparty instructing the payment before deciding to release or abort the payment.

Khan Bank also looks forward to benefiting from the **upcoming functionalities** offered by Payment Controls, which will compute statistics with pseudonymised account-level information from the entire Swift network. This will enable them to implement additional controls to detect repeated payments and new scenarios for individual accounts, as these are often indicative of fraud targeting end-customers.

Success story

“Thanks to Payment Controls, we have intercepted one phishing attempt on a customer email address and three incidents where payments were going to be sent to high-risk countries. Payment Controls’ abnormal transaction pattern detection enabled us to intercept suspicious payments which were not detected by other controls in place. Blocking such payments in real time before being released from the Swift network has prevented financial loss for the bank and its clients, but also enhanced customer experience.” – Zoltuya S., Investigation Officer, Payments and Settlement Department.

“Payment Controls also enables us to attest to the requirements within the Customer Security Programme, which mandates the implementation of transaction business controls. This will help to continue building trusted relationships with foreign correspondent banks.” – Nomulin B., Team Lead of Transaction Banking Section, Process Improvement Department.

The flexibility and ease-of-use of Payment Controls has allowed Khan Bank to change their configuration easily, rapidly, and according to their business needs. They can also easily fine-tune rules that generate false positive alerts by adapting their configuration or relying on the Rules Combination functionality.

Khan Bank are looking forward to further leveraging future developments on the Payment Controls product roadmap, informed by developments in the payments risk landscape and community feedback.

“We encourage other banks globally to adopt this powerful tool that leverages unique data to help protect the community and increase trust for partnership in payments business,” concludes Nomulin B. “Our experience adopting and using this solution has been extremely positive. Within a very short period, Payment Controls has enabled us to intercept fraudulent payments, bringing tangible benefits for our institution and customers.”

57551 - November 2022