NetRemit®

CASE STUDY

Rescuing a UK Bank's Cross Border P2P Payments Business from Legacy Security Traps

macro global®

creating value through innovation

Table of Contents

Introduction

P2P payments are gaining ground as people worldwide prefer to send and receive money safely and instantly. Thus, financial institutions are incorporating technological advancements to facilitate efficient and secure peer-to-peer (P2P) payments.

However, established financial institutions that rely on legacy systems face specific challenges following this shift. Despite the obvious convenience of P2P, robust security is essential. Legacy banking systems frequently find it difficult to keep up with the user-focused, dynamic P2P ecosystem. The old, flaw-ridden systems put the bank on a security tightrope.

A prominent foreign bank that initially positioned itself as a pioneer in facilitating cross border peer-to-peer (P2P) money transfers is the subject of this case study. Their legacy system was a major barrier, presenting notable security threats. We look at the specific security issues they ran into and how these restrictions prevented them from prospering in the changing P2P environment.

Furthermore, we shall illustrate how NetRemit, a sophisticated platform for cross-border payments, furnished the essential resources and functionalities required to traverse this delicate security zone to a safe-haven platform.

Executive Summary

An eminent foreign bank that initially thrived in the international P2P (peer-to-peer) payments space between the UK and Pakistan ultimately struggled to maintain security and growth due to its reliance on its legacy system.

This case study investigates how NetRemit, a comprehensive cross-border payment platform, surmounted the vulnerabilities and addressed the critical security challenges encountered by the foreign bank across their P2P money transfer operations.

NetRemit: A Security-Focused Solution

NetRemit's implementation went beyond simply addressing integration limitations, as the core aspect of its success lies in its robust security features, ensuring a safe and reliable P2P international remittance platform for the foreign bank.

Addressing Specific Security Challenges

The case study details how NetRemit addressed several critical security concerns:

- **Authentication:** NetRemit enforced strong Multi-Factor Authentication (MFA) to safeguard user accounts against unauthorised access.
- **OTP Management:** Secure OTP generation and storage mechanisms minimised the risk of OTP compromise and fraudulent transactions.
- **Encryption:** Implemented robust encryption protocols (like AES) to protect sensitive information during transfers, ensuring compliance with data protection regulations.
- **Communication Channels:** Secured communication channels between customer applications and the core banking system through encryption and adherence to industry standards (TLS/SSL).
- **Fraud Detection:** Advanced fraud detection algorithms with AI & machine learning capabilities enabled real-time identification of suspicious activities and fraudulent transactions.
- **Security Patches:** NetRemit's cloud-based architecture ensures automatic updates with the latest security patches, safeguarding the platform from evolving threats.
- **Scalability for Security:** Provided a cloud-based infrastructure for flexible and scalable security measures.

Outcomes and Impact

NetRemit's implementation resulted in the following significant improvements for the bank:

- Mitigated the risks associated with hacking, phishing attempts, unauthorized access, and data breaches.
- Minimized financial losses from fraudulent transactions.
- Real-time transaction monitoring and automated processes streamlined operations.
- Strong security measures fostered a secure and reliable P2P experience.
- Cloud-based infrastructure enabled the bank to adapt its security posture to meet growing demands and industry regulations.

Security as a Foundation

By prioritising security alongside other functionalities like scalability and user experience, NetRemit empowered the bank to not only recover but thrive in the competitive P2P market. Customers are more likely to engage with a platform that prioritises security measures to protect their financial data.

Client Background

A prominent foreign bank with deep roots in the UK established itself as a leader in facilitating P2P (peer-to-peer) money transfers between the UK and Pakistan, a vital financial corridor. They achieved remarkable success, processing a staggering number of transactions annually. However, their reliance on an internally developed legacy system eventually hindered their ability to maintain this level of success. While the on-premises solution served them well initially, it lacked the adaptability and robust security features needed to thrive in the dynamic financial landscape.

The legacy system presented several critical security challenges that threatened the integrity of their P2P operations in terms of OTP compromise, integration issues, limited visibility & control, and complying with the evolving regulatory landscape. These security shortcomings had a significant negative impact on the bank's P2P operations causing increased risk of fraud, loss of customer trust, security breaches and limited growth potential.

Recognising the critical need for a secure and scalable P2P solution, the bank embarked on a search for a partner that could address their security concerns and propel growth. This quest led them to Macro Global's NetRemit platform, a comprehensive solution specifically designed to optimize cross-border payment security and empower P2P transactions.

From Vulnerable to Secure: How NetRemit Fortified a Bank's P2P Payments Against Legacy System Woes

Challenge 1: Lack of Strong Multi-Factor Authentication (MFA)

The bank's legacy system allowed their users to only rely on a username and password to access their accounts and lacked robust Multi-Factor Authentication (MFA). Such logins are vulnerable to hacking or phishing attempts. Without a stronger MFA, unauthorised access to accounts becomes a significant risk. This exposed the bank to potential financial losses and eroded customer trust in its security.

Solution:

> Through multi-layered security architecture and strong customer authentication procedures like 3D authentication and Multi-Factor Authentication, NetRemit provided a safe banking system. Additional verification steps, such as OTPs delivered to users' mobile devices/email, biometric data like fingerprint verification, or security tokens, NetRemit significantly reduced the risk of unauthorised access.

Outcome:

> NetRemit's proactive approach safeguards sensitive customer data and financial information, enhancing customer satisfaction, retention rates and contributing to the bank's reputation as a trusted financial institution.

From Vulnerable to Secure: How NetRemit Fortified a Bank's P2P Payments Against Legacy System Woes

Challenge 2: Weak OTP Generation and Storage

The bank suffered from a critical weakness in how it generates and stores One-Time Passwords (OTPs) used for transaction authorisation. These temporary codes are vital for securing P2P transfers, but the existing process left them vulnerable. Such flaws in the system paved the way for malicious actors to intercept or bypass OTPs, allowing them to access customer accounts and make fraudulent money transactions.

Solution:

> Using its strong security features, NetRemit helped the bank build an extremely safe OTP generation process, which helped the bank fix this issue. The platform's unique OTP generating process assured that the codes were random, unpredictable, and resistant to hacking attempts. Furthermore, NetRemit's secure storage mechanisms effectively reduced the likelihood of unauthorised access by providing a fortified environment for storing OTPs.

Outcome:

> By addressing these vulnerabilities, NetRemit empowered the bank to enhance the security of P2P transactions, effectively safeguarding customer accounts and preventing fraudulent money transfers.

From Vulnerable to Secure: How NetRemit Fortified a Bank's P2P Payments Against Legacy System Woes

Challenge 3: Weak Encryption to Decrypt Sensitive Information

The bank's outdated system, which was dependent on basic encryption protocols, presented a major security threat on account of the likelihood of data breaches and identity theft. Cracking weak encryption methods exposes customer and financial data and violates data protection regulations.

Solution:

NetRemit employs robust encryption protocols such as AES (Advanced Encryption Standard) to encrypt sensitive information transmitted between customer interactions, ensuring end-to-end encryption. NetRemit implements secure key management practices like Hardware Security Modules (HSMs) to safeguard the encryption keys used to protect data.

Outcome:

NetRemit's robust encryption solutions assisted the bank to overcome the shortcomings of weak encryption in legacy systems and provided a more secure environment for processing P2P transactions.

From Vulnerable to Secure: How NetRemit Fortified a Bank's P2P Payments Against Legacy System Woes

Challenge 4: Insecure Communication Channels

A significant security concern for the bank stemmed from the communication channels between the customer-facing applications (mobile app and web portal) and the on-premise legacy system. These channels might have lacked proper encryption, leaving sensitive data vulnerable to interception.

Solution:

Implementation of NetRemit resolved this issue encountered by the bank through its range of security features:

- 256-bit encryption for data transmission mitigated the risk of interception and data breaches.
- End-to-end data security, utilising encryption techniques to protect data in transit and at rest, prevented unauthorised access to sensitive information transmitted between applications and the legacy system.
- Adherence to industry security standards like TLS/SSL ensured the confidentiality and integrity of data.
- Conduction of periodic vulnerability assessments and penetration testing (VAPT Testing) to identify and address weaknesses in communication channels ensured that any potential vulnerabilities are promptly mitigated.
- Secure API integration between customer-facing applications and legacy systems implemented authentication mechanisms and encryption to safeguard data exchanged through these channels.

Outcome:

NetRemit established a secure and fortified environment for data transmission, effectively mitigating the security concern related to the communication channels of the bank.

Challenge 5: Lack of Real-time Monitoring

The bank's legacy system lacked real-time transaction monitoring and thus hindered effective fraud prevention. This led to delayed detection of fraud, limited response time, and increased operational costs. This delay allowed fraudulent activities to progress, potentially causing financial losses for the bank and customers. Manual review of transactions further exacerbated the issue.

Solution:

NetRemit's seamless transaction monitoring allowed the bank to track transactions in real-time, enabling swift identification and resolution of issues. Also, the following features of NetRemit assisted the bank remarkably:

- Immediate transaction processing functionalities ensured prompt execution of transactions, enhancing efficiency.
- Transaction status updates provided instant visibility into transaction progress, aiding the bank in quick decision-making.
- Instant notification alerts inform the bank about transaction activities, facilitating timely responses.
- Live transaction reporting features offered bank with real-time access to comprehensive transaction data reports for better insights and informed decision-making.
- Accelerated fund transfer capabilities facilitated real-time fund transfers, enhancing the speed and efficiency of transactions to meet the demands of real-time transaction processing.
- The platform's dynamic transaction routing functionality allowed the bank to route transactions in real-time, optimising transaction flows and ensuring timely processing of transactions.

Outcome:

These specific features of NetRemit geared towards real-time transactions empowered the bank to streamline their transaction processes, enhance operational efficiency, and deliver superior real-time transaction services to customers.

From Vulnerable to Secure: How NetRemit Fortified a Bank's P2P Payments Against Legacy System Woes

Challenge 6: Limited Fraud Detection Capabilities

Legacy systems often lack advanced tools and analytics to identify fraudulent activity in P2P transactions, leading to security concerns. These include missed red flags, delayed detection of compromised OTPs, and increased risk of account takeover. Limited detection allows attackers to complete unauthorized transactions before flagging them, allowing them to steal money.

Solution:

NetRemit's advanced fraud detection algorithms analysed transaction patterns, using machine learning and artificial intelligence, improving the accuracy in detecting fraudulent behavior.

NetRemit automated the process of identifying red flags or suspicious transaction patterns promptly, flagging high-risk transactions for further investigation. The platform leveraged behavioral analytics to monitor user activities and identify deviations from normal patterns, enabling the detection of suspicious activities in real-time.

Outcome:

NetRemit enabled the bank to efficiently identify fraudulent transactions and immediately intervene to prevent them and minimise financial losses, without causing delays in legitimate transactions.

Challenge 7: Overhead Expenses

The bank faced a significant security risk as they lack the agility to receive regular updates, creating vulnerabilities for attackers to exploit. These vulnerabilities led to data theft and disruption of operations. Additionally, they were more susceptible to malware infections and non-compliance penalties.

Solution:

NetRemit significantly enhanced the security and integrity of the bank's cross-border payment infrastructure through its range of features:

- NetRemit incorporates a highly advanced security architecture that includes the latest security patches and updates to combat evolving security threats.
- Fully compliant with ISO & OSWASP standards, ensuring that security protocols and best practices uphold the highest industry standards.
- Leveraging the expertise of technology partner Microsoft and the hosted platform Azure, NetRemit offers enterprise-grade security that includes multi-factor authentication, secure data capture, stringent data retention policies, malware protection, robust encryption, and periodic vulnerability assessments.
- Employs IP restrictions to control access to the admin portal, adding an extra layer of security to restrict unauthorized access attempts.
- Align with regulatory requirements and support secure data lifecycle management.
- Comes with an inbuilt incident management system that allows for the timely and effective response to security incidents, ensuring rapid resolution and mitigation of any identified vulnerabilities.

Outcome:

NetRemit effectively addressed this challenge, providing a comprehensive and proactive security framework for the bank, safeguarding the integrity of cross-border payment transactions.

From Vulnerable to Secure: How NetRemit Fortified a Bank's P2P Payments Against Legacy System Woes

Challenge 8: Limited Scalability for Security Measures

The bank's on-premises legacy system presents challenges in implementing robust security measures due to resource constraints, compatibility issues, limited agility, and increased risk of security breaches. These limitations create vulnerabilities and limit the bank's ability to deploy advanced security tools effectively.

Solution:

NetRemit addressed these limitations by offering a cloud-based solution. By leveraging the cloud, NetRemit provided a scalable and flexible infrastructure for the bank to deploy advanced security measures without the traditional resource constraints and compatibility issues associated with on-premises systems.

Through the NetRemit Admin Center, the bank gained the power to configure and control business rules, including security validations, fraud screening parameters, access control, and more. This enables the effective deployment of security measures that can adapt to the bank's growing needs, compensating for the limitations of the legacy system's agility in deploying advanced security tools.

Outcome:

NetRemit's cloud-based infrastructure and dynamic configuration and control capabilities empowered the bank to deploy advanced security tools, mitigate vulnerabilities, and enhance its security posture based on its size across its cross-border payment operations.

Results and Impacts

NetRemit's implementation yielded significant improvements in security, efficiency, and customer trust for the foreign bank's international remittance business. Here's a breakdown of the key results and impacts:

Significantly minimised the chances of successful hacking or phishing attempts.

Robust storage mechanisms to safeguard OTPs reduced the likelihood of unauthorized access and prevented fraudulent money transfers.

Strong encryption algorithms made it significantly harder for attackers to decrypt information even if they breach the system.

Encryption practices help the bank comply with data protection regulations that mandate strong encryption for sensitive data.

Implementation of secure communication protocols between customer applications and the core banking system mitigated the risk of interception.

Real-time monitoring enables prompt detection and reaction to suspicious activity, thereby averting fraudulent transactions.

Efficient and economical processes resulted from the elimination of manual transaction evaluation through automated monitoring.

The bank can reduce financial losses from fraud by identifying red flags and suspicious behaviour through the analysis of transaction patterns using AI-powered algorithms and machine learning.

Automated updates with the most recent security patches are sent to the platform using cloud-based architecture, protecting it from ever-changing threats.

Allow the bank to scale its security measures as needed, adapting to growth and deploying advanced security tools effectively.

Conclusion

The case study demonstrates the successful migration of a prominent foreign bank's P2P (peer-to-peer) money transfer system from a legacy system to NetRemit. This transition resulted in substantial security improvements, enhanced efficiency, and a more robust foundation for future growth.

NetRemit addressed the critical security vulnerabilities of the legacy system through a multi-pronged approach. This included implementing strong Multi-Factor Authentication (MFA), secure OTP generation and storage, robust encryption protocols, and secure communication channels. Additionally, NetRemit's real-time transaction monitoring, advanced fraud detection capabilities, and automatic security updates further bolstered the bank's security posture.

Beyond security, NetRemit's cloud-based architecture offers scalability and flexibility, allowing the bank to adapt its security measures as needed. This empowers them to keep pace with evolving threats and industry regulations.

Thus, by prioritizing security and leveraging cutting-edge technology, NetRemit empowered the bank to deliver a secure and efficient P2P money transfer experience for its customers.

We are here to help you

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

https://www.macroglobal.co.uk/contact-us/

macro global®
creating value through innovation

Macro Global (MG) is the trading name of Macro Infotech Limited, Inca Infotech Ltd & Macro Technology Solutions Pvt Ltd. Macro Infotech Limited & Inca Infotech Limited have Registered Office at 25, Cabot Square, Canary Wharf, London – E14 4QZ and these companies are registered in England & Wales under the registration number 06477763 & 04017901.

Technology Partnerships

Microsoft Gold Partner

amazon web services Partner Network
TECHNOLOGY PARTNER

trust payments

kaleyra

ISO Certifications

ISO 9001:2015 Quality Management System Cert. #: 0922900102

ISO 27001:2013 Information Security Management Cert. #: 09222700102

ISO 27701:2019 Privacy Information Management Cert. #: 09222770102

ISO 27018:2019 PII Protection in Public Clouds Cert. #: 09222701802