LexisNexis®
RISK SOLUTIONS

CASE STUDY

LexisNexis® ThreatMetrix® Helps Qudos Bank Identify Hard-to-Detect Scams and Remote Access Attacks, Preventing ~$350,000 of High-Risk & Fraudulent Money Transfers

AT A GLANCE

CUSTOMER

Qudos Bank

REQUIREMENTS

- Protect customers and their accounts by detecting the full spectrum of scams.
- Reduce fraud losses.
- Improve operational efficiencies.

SOLUTION

With LexisNexis® ThreatMetrix®, Qudos Bank is able to reliably detect high-risk and fraudulent transactions across logins, payments and password reset customer touchpoints, in near real time. Qudos Bank collaborated closely with the ThreatMetrix professional services team, using its collective expertise as an extension of the bank's fraud operations, in order to optimize the fraud detection rate and reduce manual reviews.

BOTTOM LINE

- Enhanced fraud detection and risk-based decisioning, detecting approximately $350,000 of high-risk and fraudulent money transfers related to scams.
- Recognized more customers as trusted, reducing manual reviews.
- Maintained low average reject rate, increasing efficiency of fraud operations.
- Developed a proactive fraud strategy, working with ThreatMetrix professional services to respond quickly to new and emerging attack patterns and trends.

CASE STUDY

"We weren't just looking for a point solution or security vendor. We wanted a technology partner and we found that with LexisNexis® ThreatMetrix®. The professional services team is exceptional — listening to our feedback and collaborating on optimizing our fraud strategy."

— ANTAR CHAHINE, CHIEF RISK OFFICER – QUDOS BANK

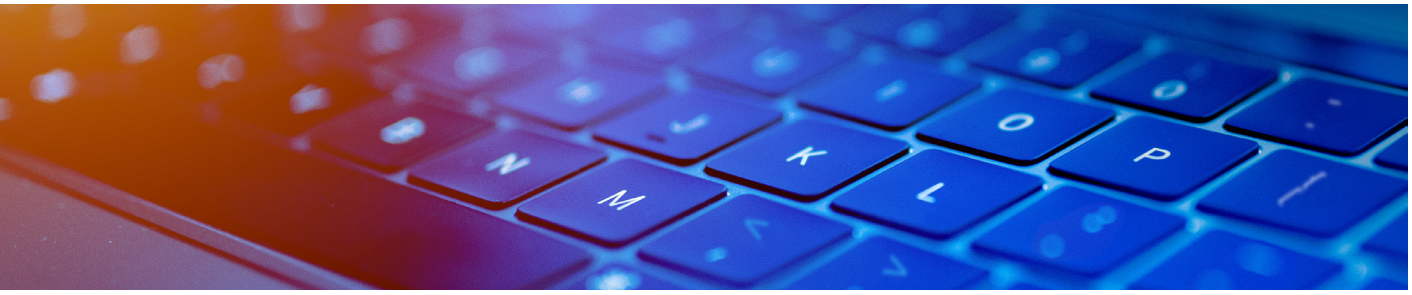
From Small Credit Union to One of Australia's Largest Mutual Banks

Qudos Bank is one of Australia's largest mutual banks with over 96,000 members across Australia. Founded as Qantas Credit Union in 1959 by a group of Qantas employees, Qudos Bank has grown to become an award-winning financial services provider for all Australians.

Positioned as 'the bank you can rely on, at any time of life', Qudos Bank is committed to creating mutual value through empowering customers, better products and outstanding service. The customer is at the heart of Qudos Bank, with the way in which the bank operates designed to benefit customers first.

Financial Services — A Prime Target for Fraudsters Armed with Remote Access Trojans (RATs)

The customer is fast becoming the weakest link in cybersecurity, with fraudsters increasingly looking to socially engineer victims with promises of financial gain or securing a hacked account. Using sophisticated ruses and phishing techniques, fraudsters trick customers into divulging credentials, installing malware or transferring money.



Like other financial institutions, Qudos Bank customers were being targeted by fraudsters using different methods and scams, including:

- **Investment and Employment Scams:** Fraudsters trick customers into transferring money by offering an investment or job which is 'guaranteed' to make fast money or land a high-paying job for little or no effort.
- **Remote Access Attacks:** Fraudsters, via methods such as social engineering, use remote access software to infiltrate and take over customer accounts. Once the fraudster has gained control of the account, the fraudster changes the beneficiary details or sets up a new payment in order to exfiltrate funds. In one attack, Qudos Bank customers were being targeted by fraudsters posing as trusted Australian telecommunication providers, with the fraudsters asking customers to install remote access software in order to facilitate fraudulent money transfers.
- **Dating and Romance Scams:** This type of scam is a confidence trick, with fraudsters feigning romantic intentions towards a victim. Once the fraudster has gained the victim's trust, they then manipulate the affections of the victim in order to commit fraud.
- **Phone Porting:** A fraudster, armed with stolen credentials or information specific to the targeted customer, will phone the mobile network provider and ask for the victims' number to be moved to another network via the Porting Authorization Code (PAC). Now in control of the mobile number, the fraudster can take advantage of a weakness in two-factor authentication, whereby the second factor is a text message or a call to a mobile number.

"The ThreatMetrix solution gives us the ability to see the very early warning signs of a possible scam — be it a remote access software installation or a payment to a new beneficiary. Being able to detect changes in legitimate customer behavior gives us the edge in the fight against social engineering."

— ANTAR CHAHINE, CHIEF RISK OFFICER – QUDOS BANK

CASE STUDY

Using Digital Identity Intelligence to Enhance Authentication and Fraud Decisioning in Financial Services

The LexisNexis® ThreatMetrix® solution brings unparalleled intelligence to the entire customer journey, with digital identity intelligence revolutionizing the traditional identity challenges faced by Qudos Bank – intrusive step-up, siloed policies, limited visibility and static data.

The LexisNexis® Digital Identity Network® collects and processes global shared intelligence from millions of daily consumer interactions including logins, payments, and new account applications. Using this information, the ThreatMetrix solution creates a unique digital identity for each user by analyzing the myriad connections between devices, locations, and anonymized personal information. Behavior that deviates from this trusted digital identity can be reliably identified in near real time, alerting Qudos Bank to potential fraud.

This intelligence can be used to detect patterns of high-risk behavior associated with scams and remote access attacks, detecting changes in normal customer behavior such as the first installation of remote access software, followed by a payment to a new beneficiary.

Working closely with the professional services team, Qudos Bank was also able to streamline and enhance internal fraud operations; the bank saw reduced calls to the contact center, as well as significant time efficiencies with the manual review process automated. Collaborating with ThreatMetrix professional services, Qudos Bank was able to take a more proactive approach to fraud detection; professional services helped the bank to identify approximately 50 customers who had had their credentials and accounts compromised. Qudos Bank was able to take pre-emptive action with regard to the compromised accounts, resetting the customers' passwords before any fraud had occurred.

The Fraud Tools Used By Qudos Bank To Better Protect Customers

Qudos Bank leverages a number of key LexisNexis® ThreatMetrix® features to help support its strategy for protecting customers and reducing fraud and streamlining operational efficiencies, including:

ThreatMetrix Mobile: A lightweight software development kit (SDK) for Google Android and Apple iOS mobile devices, providing complete fraud protection for the mobile channel. This includes application integrity evaluation, advanced persistent device identification, malware detection, location services, jailbreak and root detection technologies, anomaly and device spoofing detection and dynamic configuration and updates.

Smart Rules: These help Qudos Bank to better understand genuine customer behavior, while reliably detecting genuine fraud. The ThreatMetrix solution uses behavior, age and location to examine the historical data related to a given transaction, in order to run a deep behavioral assessment. This helps the bank to more reliably differentiate between true fraud and legitimate behavior change, reducing the step-up frequency without increasing overall risk.

Trust Tags: Enable the bank to differentiate between fraudsters and legitimate users by dynamically associating any combination of online attributes involved in accepting, rejecting or reviewing a transaction. Trust Tags act as digital labels that can be applied to various combinations of entities within a user's persona to indicate their trustworthiness, reducing friction for legitimate users and more reliably identifying high-risk behavior.

CASE STUDY

Champion Challenger: This capability helps Qudos Bank to determine the effectiveness of policy changes and fine tune policies to keep pace with changes in consumer behavior and to stay ahead of emerging fraud patterns.

ThreatMetrix Professional Services: The team provides a full portfolio of professional services to expertly guide any business, of any size, through the design, implementation and ongoing optimization of best in class fraud, identity and authentication solutions. The team of experts within professional services work collaboratively with Qudos Bank to help maximize the ongoing effectiveness and value of the ThreatMetrix solution.

"Fraudsters never stop innovating – trying to find new weak points or fraud MOs — so we should never stop innovating either. With ThreatMetrix, we have the intelligence and industry expertise to anticipate and prepare for certain trends or attacks. We can then build flexible rules which can be quickly deployed if we see that attack pattern in the wild."

— ANTAR CHAHINE, CHIEF RISK OFFICER – QUDOS BANK

LexisNexis® RISK SOLUTIONS

For more information, visit risk.lexisnexis.com/global/en