INVESTIGATING DATA ANOMALIES IN BRAZIL

JUNE 2024

Executive summary

- The Data team have discovered an increase in fraudulent transaction attempts in Brazil during the period May 2023 - June 2023. The uptick appears have stemmed from Nu Pagamentos SA Bank.

- This could be because the bank has been expanding rapidly which may have led to gaps in their fraud detection mechanisms or it may have been a targeted attack. This may have resulted in customer data being stolen.

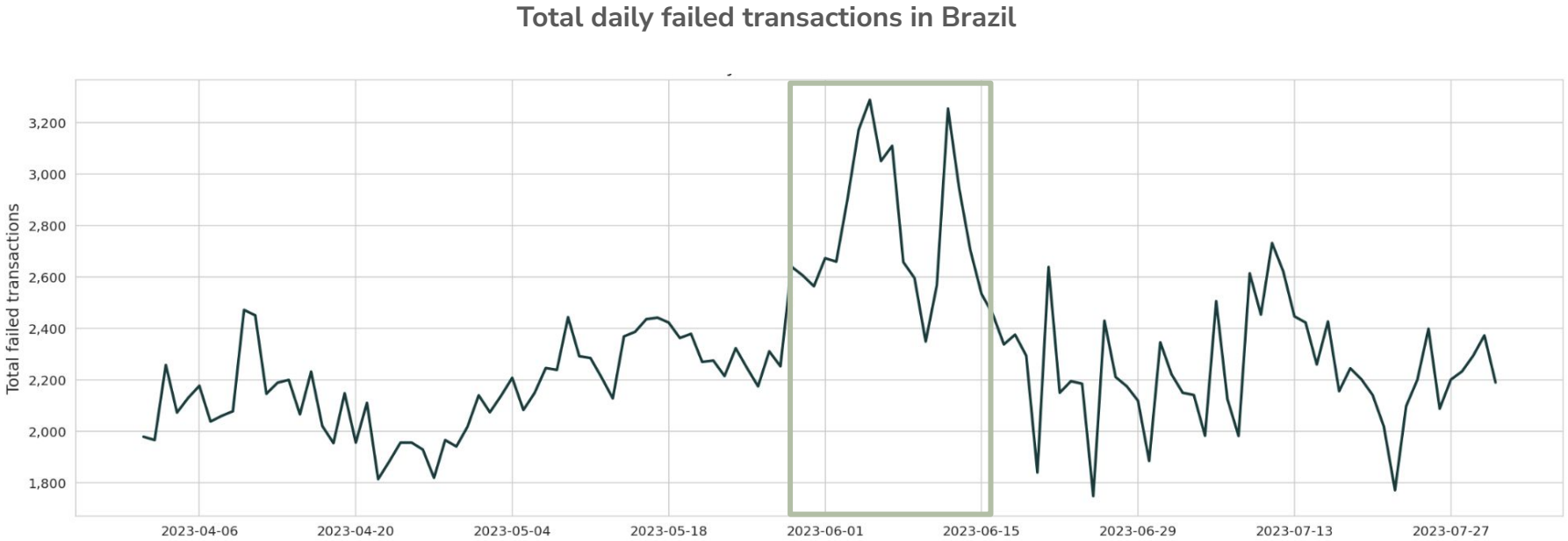
- In the immediate term, we recommend:
  - Contacting the bank to make them aware of the issue
  - Increasing our own security checks of transactions coming through from this bank
  - Notifying affected customers and encouraging them to change their passwords

- In the medium and longer term, we recommend:
  - Using advanced machine learning models to predict and prevent future fraud attempts
  - Investing in advanced fraud detection tools such as AI driven anomaly detection
  - Strengthening overall cybersecurity infrastructure, including encryption and secure APIs

Background

- The Data team have recently discovered a concerning anomaly in the Brazil market data.
- The following slides show an increase in fraudulent transaction attempts in this market during the period May 2023 - June 2023.
- The uptick appears to be stemming from a single bank.
- The presentation concludes with an action plan for next steps.

Failed transactions spiked in Brazil in the first half of June 2023

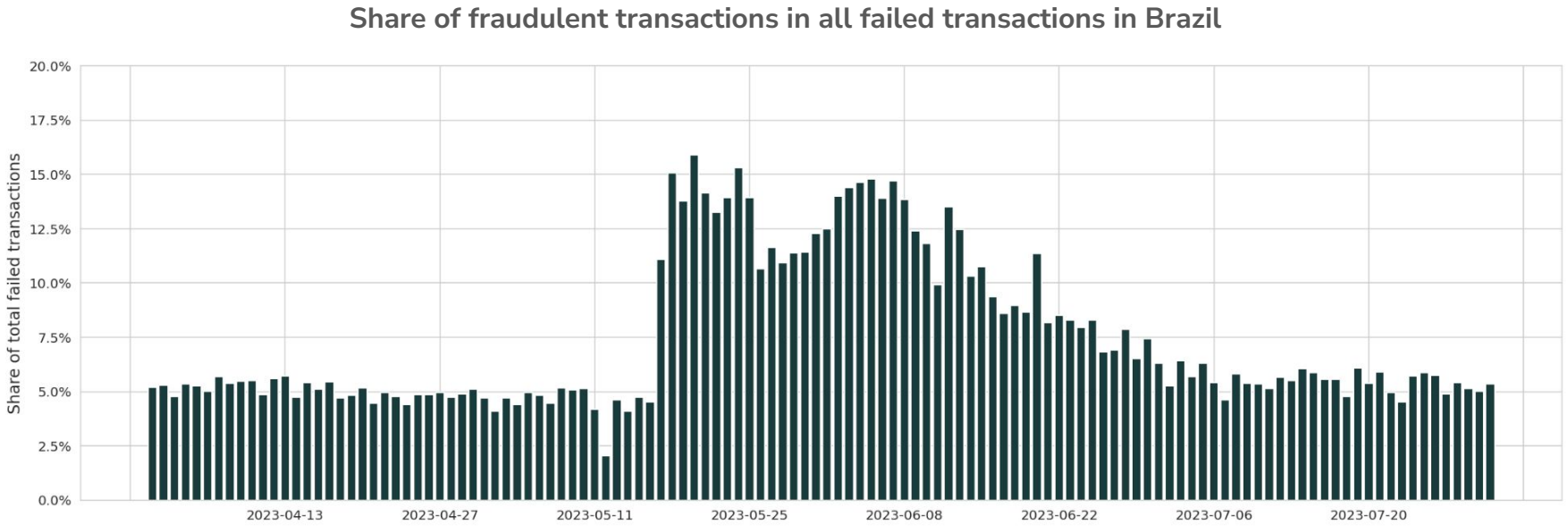


The uptick in failed transactions appears to be due to an increase in fraudulent transaction attempts

- When looking at fraud in isolation, we see an additional spike in activity in the second half of May 2023.

Fraudulent transaction attempts increased as a share of all failed transaction attempts during the period in question

- The share of fraudulent transaction attempts in all failed attempts increased from circa 5% in April 2023 to 13-15% in May/June 2023.



The increase in fraudulent transaction attempts appear to stem from a single bank: Nu Pagamentos SA Bank

- Nu Pagamentos SA Bank is the world's largest digital banking platform outside of Asia, serving over 100 million customers across Brazil, Mexico, and Colombia.
- Whilst we did see an increase in fraudulent transaction attempts in May/June, the company seems to have got this under control in the months since.

Total daily failed transactions attributed to fraud at Nu Pagamentos SA Bank

Why are we seeing these trends?

- Nu Pagamentos SA Bank has been expanding rapidly which may have led to gaps in their fraud detection and prevention mechanisms.
- As part of their growth, certain marketing promotions may have attracted legitimate customers as well as fraudsters.
- The timing tied in with the holiday season which typically results in an increase in online transactions. This may have provided more opportunities for fraudsters.
- There may have been a targeted attack at the bank which may have resulted in fraudsters exploiting vulnerabilities in security systems and stealing customer data.

Actions and recommendations: Immediate term

- Contact Nu Pagamentos SA Bank to report the issue and share detailed information of the patterns and transactions involved.
- Work with the bank to identify and close security gaps.
- Increase our own scrutiny of transactions from Nu Pagamentos SA Bank and use more stringent fraud detection algorithms.
- Implement real-time alerts for suspicious activities linked to transactions from this bank.
- Notify affected customers about the issue and advise them on steps to secure their accounts, such as changing passwords and monitoring transactions.

Actions and recommendations: Medium and longer term

- Perform a detailed analysis of fraudulent transactions to identify trends and improve existing fraud detection models.
- Use advanced machine learning techniques to predict and prevent future fraud attempts.
- Invest in advanced fraud detection tools and technologies, such as AI-driven anomaly detection and blockchain for transaction verification.
- Strengthen overall cybersecurity infrastructure, including encryption, secure APIs, and regular updates.
- Conduct regular security audits of our transaction processes and third-party integrations.

THANK YOU