**Portfolio Piece 2: Problem Solving and Continuous Improvement**

**Executive Summary**

This report details my involvement in resolving a significant data quality issue within Lloyds Banking Group’s Consumer Relationships division. The incident involved customer contact details being overwritten due to imposter fraud applications. Working collaboratively across teams, I contributed to root cause analysis, remediation planning, and the implementation of improved controls. The project demonstrates my problem-solving skills, application of continuous improvement principles, and effective use of enterprise data governance tools.

**Introduction**

This submission builds directly on feedback received from my formative assessment. I was advised to focus on a work-based project and to deepen my critical reflection. Accordingly, I have selected a real incident from my role as a Data Quality Analyst, ensuring stakeholder involvement and practical impact.

In February 2024, a customer reported an incorrect telephone number on their profile. Investigation revealed this was due to a fraudulent credit card application processed via an unauthenticated channel. Although the fraud was detected and the application rejected, the customer’s contact details were inadvertently updated with those provided by the fraudster. This issue highlighted a gap in the data update process and prompted a wider review of similar incidents.

**Background and Context**

Lloyds Banking Group processes large volumes of credit card applications daily, relying on automated data pipelines and fraud detection systems. The Online Customer Information System (OCIS) serves as the central repository for customer data, supporting multiple business functions. The incident exposed a flaw in the integration between unauthenticated sales channels and OCIS, where rejected applications could still trigger updates to customer contact information.

Issue management and remediation tracking were conducted using Collibra, the Group’s enterprise data governance platform. This ensured transparency, accountability, and cross-team collaboration throughout the lifecycle of the issue. Collibra provided a centralised record of the issue’s discovery, root cause analysis, remediation planning, and business impact assessment. The platform enabled cross-team collaboration and ensured that all actions were documented and auditable.

**Methodology**

**1. Identifying and Scoping the Problem**

The issue was initially raised by the Private Banking team and subsequently confirmed through analysis of application and customer data. Collibra records indicated similar instances had been previously reported, prompting a comprehensive review of the affected processes. The frequency of occurrence was found to be daily, with both ongoing and historical data affected. This highlighted the need for urgent remediation to prevent further customer impact.

**2. Root Cause Analysis**

Root cause analysis established that when an application was marked as ‘imposter’ and rejected, there were no additional checks to prevent customer data from being overwritten. The flaw was traced to the business process and system logic between the unauthenticated sales site and OCIS. Analysis identified multiple instances of data overwriting, with both ongoing and historical data affected. The root cause was classified as a business process not driving the correct data update, and the issue was categorised under the data quality dimension of accuracy.

**3. Collaborative Problem Solving**

A cross-functional team, including Fraud & Disputes, Data Quality, and platform engineers, worked together to map the process, validate findings, and design remediation steps. Stakeholder engagement was facilitated via Collibra, ensuring all actions and decisions were documented. The team held workshops to map every step of the credit card application pipeline, using process flow diagrams to visualise the journey and identify gaps. This collaborative approach ensured that all perspectives were considered and that the solution addressed the root cause effectively.

**4. Remediation and Monitoring**

Remediation involved updating system logic to ensure unauthenticated journeys pass the correct System ID to OCIS, preventing unauthorised updates. The OCIS Shield control was implemented to block changes from unauthenticated sources, with full coverage scheduled for August 2025. Ongoing monitoring and reporting were established to detect and prevent future occurrences. Automated dashboards were created to provide real-time visibility of incidents, and alerts were set up to notify the data quality team of any anomalies.

**Results and Findings**

* **Incident reduction:** The implementation of new controls has significantly reduced the frequency of data overwriting incidents. Analysis identified 18 instances of data overwriting in credit card applications between January and February 2024, but since the deployment of the fix, incidents have dropped to near zero.
* **Customer experience:** Improved accuracy of contact data has enhanced customer trust and reduced complaints. Customers are now less likely to experience issues with authentication or receive communications intended for others.
* **Operational efficiency:** Automated controls have minimised manual interventions and improved data integrity. Contact centre staff no longer need to manually correct customer details, freeing up resources for other tasks.
* **Business impact:** The issue was classified as ‘Material’ for customer, regulatory, and reputational risk, with minor financial loss. Remediation aligns with Consumer Duty and regulatory requirements, reducing the likelihood and severity of future incidents.

**Reflection and Lessons Learned**

This project reinforced the importance of robust data governance and cross-team collaboration. Key lessons include:

* **The value of enterprise tools:** Collibra proved invaluable for issue management, providing a single source of truth and enabling effective collaboration across teams. The ability to track progress, document decisions, and maintain an audit trail was critical to the success of the project.
* **Continuous monitoring:** The incident highlighted the need for ongoing monitoring and regular process reviews to identify and address emerging risks. Automated dashboards and alerts have become standard practice, enabling proactive management of data quality issues.
* **Stakeholder engagement:** Engaging stakeholders from across the business ensured that the solution was comprehensive and addressed the needs of all affected parties. Regular updates and transparent communication helped build trust and secure buy-in for the remediation plan.
* **Documentation and knowledge sharing:** Documenting the process and sharing lessons learned has helped inform future improvements and prevent recurrence of similar issues. The experience has also contributed to the development of best practices for data quality management within the organisation.

**Critical Reflection**

While the remediation addressed the immediate issue, alternative approaches such as manual approval for all flagged applications were considered. The chosen solution balanced operational efficiency and risk mitigation, but ongoing vigilance is required to ensure controls remain effective as processes evolve. It is important to regularly review and update controls in response to changes in the business environment, regulatory requirements, and emerging threats.

The project also highlighted the importance of critical reflection and continuous improvement. By evaluating the pros and cons of different approaches, the team was able to select the most effective solution while minimising disruption to business operations. This experience has reinforced the value of critical thinking and adaptability in problem-solving.

**Continuous Improvement**

The incident prompted a review of related processes and the implementation of enhanced survivorship rules for customer data updates. Regular risk assessments and process mapping are now standard practice, supported by automated monitoring and reporting. The team has also explored the use of new technologies and methodologies, such as anomaly detection tools and machine learning algorithms, to further improve data quality and prevent future incidents.

Continuous improvement is embedded in the organisation’s culture, with a focus on learning from past experiences and proactively identifying opportunities for enhancement. The lessons learned from this project have been shared across teams, contributing to a culture of collaboration and innovation.

**Recommendations**

* **Standardise process mapping and documentation** for all new projects to ensure transparency and facilitate early identification of potential risks.
* **Encourage peer review and cross-team collaboration** to leverage diverse expertise and perspectives in problem-solving.
* **Leverage enterprise data governance tools** like Collibra for issue tracking, remediation, and auditability.
* **Continue to monitor and refine controls** to adapt to changing business and regulatory requirements.
* **Invest in training and knowledge sharing** to build data quality awareness and capability across the organisation.
* **Explore new technologies and methodologies** to enhance data quality management and support continuous improvement.

**Conclusion**

This experience demonstrated the impact of a single process flaw on customer trust and business operations. By applying structured problem-solving, leveraging data governance tools, and collaborating across teams, we delivered a sustainable solution and strengthened our approach to data quality management.

The project has also contributed to my personal and professional development, enhancing my problem-solving skills, technical knowledge, and ability to work effectively in cross-functional teams. I have gained a deeper understanding of the importance of data quality, governance, and continuous improvement in supporting business objectives and delivering value to customers.

**Appendix – Supporting Evidence**

* Process flow diagrams and monitoring dashboard screenshots (all anonymised and compliant with data protection standards).

A diagram of a credit card application

AI-generated content may be incorrect.

* Collibra issue management summary (with sensitive information redacted).

A screenshot of a computer

AI-generated content may be incorrect.

* Meeting notes and workshop outputs demonstrating cross-team collaboration. **(anonymised)**

A screenshot of a phone number data issue

AI-generated content may be incorrect.