How to Safely Update Counterparty Addresses in FIS Quantum Without Wiping Identifiers

A practical guide to avoiding silent data loss during bulk updates in live treasury environments

Bisi Tishe · Lumin Treasury Consulting · April 2026

Updating counterparty data in FIS Quantum is often treated as routine. In practice, it carries more risk than most teams expect.

What looks like a straightforward address update can result in unintended changes to other fields — particularly identifiers such as SWIFT codes, LEIs, or internal reference codes. The difficulty is that these issues are not always immediately visible. The import completes successfully, no error messages appear, but the underlying data has quietly changed in ways that were never intended.

This guide sets out a practical approach to updating counterparty address data safely, based on direct experience working with live Quantum environments.

The core problem: bulk updates are not always incremental

When working with JSON imports in Quantum, the system does not merge all fields — some fields are replaced entirely. This is particularly relevant for structured fields such as identifiers and analysisCodes.

If these fields are included in the import payload, they are treated as a complete replacement, not a partial update. Any mismatch in structure or naming can result in data being removed or overwritten without warning.

> ***Example risk***
>
> *Including the following in a JSON payload:*
>
> `"identifiers": {}`
>
> *does not mean "leave identifiers unchanged". It means: clear all existing identifiers for that counterparty.*
>
> *This behaviour is not always obvious — and can lead to silent data loss in a production environment.*

Why address updates can trigger wider issues

Address updates are typically sourced from external or business-owned data — often an Excel file. To apply them, teams usually follow a straightforward process: export a JSON file from Quantum, merge the updated fields into it, and re-import. The risk sits in step two.

If the merged file includes fields beyond the intended update scope, those fields may also be affected during import. Common issues include:

- Identifiers being overwritten due to structure mismatch
- Field names not matching system configuration — for example, using a label rather than the internal name
- Fields being included in the payload that were never intended to be part of the update

---

The safer approach: treat updates as targeted patches

The most effective way to reduce risk is to minimise the scope of the update file. Rather than treating the import as a full record update, treat it as a targeted patch — only the fields that need to change should be in the file.

What to include:

- Only the fields being updated
- The required import structure — application, action, identifier, data block

What to exclude unless explicitly part of the update:

- identifiers
- analysisCodes
- Any structured field not part of the intended change

A recommended process

A controlled update process typically follows these steps:

1. Export baseline data from Quantum

This gives you the correct record structure and identifiers to work from.

2. Prepare update values in Excel

Include only the fields requiring updates — for example, postalAddress fields only.

3. Convert the update file to CSV

Use a structured, clean format for transformation into JSON.

4. Apply updates to the JSON structure

Match records using the identifier. Update only approved fields. Remove everything else.

5. Rebuild a minimal JSON file

The final payload should contain only the fields necessary for the update — nothing more.

6. Validate before import

Check record counts. Review sample records. Confirm that excluded fields are not present in the file.

7. Test on a small batch first

Always validate against a limited set of records before running the full production upload.

> ***A practical observation***
>
> *In most cases, the safest file is not the most complete one — it is the simplest one. Reducing the payload to only the necessary fields reduces the chance of unintended updates, improves transparency, and makes validation far easier. Less is genuinely more when working with live production data.*

Closing thought

Bulk updates in treasury systems are rarely complex from a technical standpoint. The challenge is control.

Understanding how Quantum handles data structures — particularly the difference between replacement and merge behaviour — is critical when working in production environments. Address updates may seem low risk, but without a disciplined approach, they can affect far more than intended.

A minimal, targeted, well-validated process ensures that only the intended fields are updated, existing data remains intact, and operational risk stays where it belongs — managed rather than discovered.

> If you are working with FIS Quantum and dealing with similar data update challenges, feel free to get in touch at info@lumintreasury.com or connect on LinkedIn. Always interested to hear how others are approaching this in live environments.

Lumin Treasury Consulting · Independent Treasury Technology Advisory · lumintreasury.com · info@lumintreasury.com