PMPG
Payments Market Practice Group

NOVEMBER 2023

Ultimate Parties in Cross-Border Payment Messages

Market Practice Guidelines

DISCLAIMER

Whilst the Payments Market Practice Group (PMPG) has used its best endeavours to make sure that all the English information, data, documentation and other material (copy and images) in this document are accurate and complete, it does not accept liability for any errors or omissions.

The PMPG, or any of its members, will not be liable for any claims or losses of any nature arising directly or indirectly from use of the information, data, documentation or other material in this document.

Links from this document to other sites are for information only. PMPG accepts no responsibility or liability arising from access to, or for the material on, any site to which it is linked, nor does the presence of links to other sites imply any endorsement by PMPG of these sites or their contents.

Reproduction, redistribution and transmission of any information, data or other material contained in this document is permitted, as long as its source is acknowledged.

Proceeding to read this document is confirmation that you have understood and accepted these terms.

Payments Market Practice Group

The Payments Market Practice Group (PMPG) is an independent body of payments subject matter experts from Asia Pacific, EMEA and North America.

The mission of the PMPG is to:

- Take stock of payments market practices across regions.
- Discuss, explain, and document market practice issues, including possible commercial impact.
- Recommend market practices, covering end-to-end transactions.
- Propose best practice, business responsibilities and rules, message flows, consistent implementation of ISO messaging standards and exception definitions.
- Ensure publication of recommended best practices.
- Recommend payments market practices in response to changing compliance requirements.

The PMPG provides a truly global forum to drive better market practices, which, together with correct use of standards, will help in achieving full straight-through-processing and improved customer service.

Follow us on LinkedIn

Contents

1 Executive Summary

With various market infrastructures and Swift moving to the ISO 20022 messaging standard, the global payments industry stands to gain from enhanced data richness, structure and transparency.

Amongst the payment scenarios that benefit from the enhanced data elements introduced with ISO 20022, are the so-called payments/collections “on behalf of” (POBO / COBO). These transactions are executed by a third party on behalf of the ultimate payer and/or beneficiary and require the specification of an ultimate debtor and/or ultimate creditor in a payment message.

As opposed to legacy FIN MT messages, which do not carry dedicated fields to provide information on the ultimate parties of a payment, ISO 20022 offers clear structure and designated data elements, allowing remitters to clearly identify ultimate parties, thereby improving the creditor’s reconciliation and interbank anti-financial crime processes.

Nonetheless, to fully realize the benefits of the ISO 20022 standard, payment messages and their respective data elements must be populated in line with the ISO 20022 definition. Incorrect population of ultimate party information is associated with manual intervention, investigations and may result in subsequent delays in payment processing and increased costs.

Furthermore, given that ultimate parties are defined as sensitive payment information, their correct identification and provision in payment messages is particularly important for anti-financial crime controls. Any non-compliance (for instance, concealing of the ultimate beneficiary/creditor details) is subject to regulatory consequences. This is also reflected in the revised Wolfsberg Group Payment Transparency Standards.[1]

Early days of the ISO 20022 migration have shown that new data elements introduced with ISO 20022, such as ultimate parties, often become subject to misinterpretation and incorrect provision of the information, leading to reconciliation issues and compliance concerns.

Amongst most prominent use cases of non-compliance, observed by the global payments community, are the following:

- Duplication of the debtor/creditor details in the corresponding ultimate party elements.
- Product name/brand supplied as part of ultimate party details.
- Details on debtor/creditor department provided as ultimate party information.
- Provision of ultimate party information with “NOTPROVIDED” as the data value.
- Capture of payment service providers (PSPs) as debtor / creditor with underlying customer as an ultimate party.

With the aim of helping guide the industry on the correct usage of the ISO 20022 standard, this paper shares market practice guidelines on the provision of ultimate party data elements within ISO 20022 messages to support on-behalf-of payment scenarios.

Following the outlined guidelines and ensuring high levels of data quality supplied in ISO 20022 payment messages will help the industry achieve faster, better and more transparent payments.

[1] Wolfsberg Group Payment Transparency Standards 2023.pdf (wolfsberg-group.org)

2 Introduction

From enabling new levels of transaction data richness, structure and transparency, to opening up opportunities for new business offerings, the ISO 20022 messaging standard brings clear benefits to the payments industry.

Amongst payment scenarios that look to benefit from the enhanced compliance are so-called payments and collections/receivables “on behalf of” (POBO & COBO/ROBO), which require the specification of a debtor and/or ultimate debtor, and creditor and/or ultimate creditor. In a payment factory scenario, for example, while a payment may be credited to a head office’s account (creditor), the ultimate beneficiary of the payment may be a subsidiary of the company (ultimate creditor) instead.

Ultimate debtor:

Represents a party that originally ordered goods / services and to whom the seller has sent the invoice. Ultimate debtor is used when the receiver of the invoice is different from the payer.

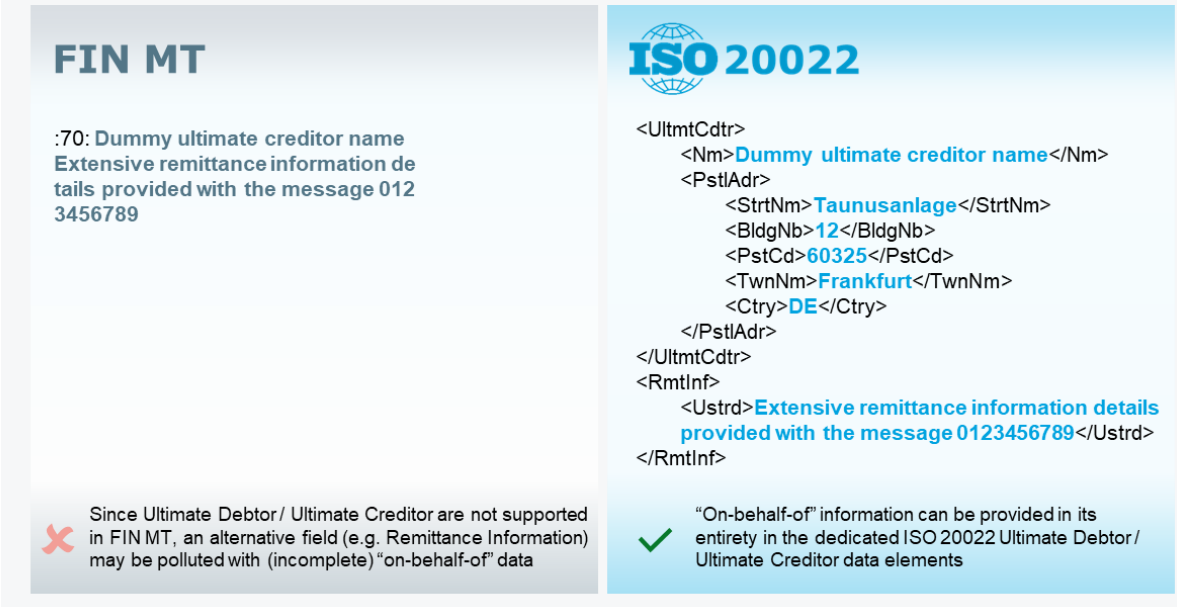
Ultimate creditor:

Represents a party that is the ultimate beneficiary of the payment. For example, the payment is credited to an account of a financing company, but the ultimate beneficiary is the customer of the financing company.

Given that legacy FIN MT messages do not have a designated field for identification of ultimate parties, this information is often being transported in an alternative field, for instance, remittance information. This makes it difficult to ensure that all relevant data is passed down the payment chain, meaning that information can be either excluded, or truncated and added to another field, where it might be overlooked in screening, often delaying payment processing and complicating reconciliation.

The ISO 20022 messaging standard, on the other hand, introduces specific data elements for this purpose – ultimate debtor and ultimate creditor – which address issues of the legacy FIN MT and help to improve reconciliation processes and anti-financial crime controls.

Figure 1: Ultimate parties in FIN MT vs ISO 20022 (Source: PMPG)



Nonetheless, whilst the clean representation of such payment scenarios is supported by the ISO 20022 messaging standard, ultimately it comes down to the correct population of the payment messages. As the early days of the ISO 20022 migration have shown, new data elements introduced with ISO 20022, such as ultimate parties, often become subject to misinterpretation and incorrect provision of the information, leading to compliance and reconciliation concerns.

This paper aims to help and provide guidance to the industry on the correct usage of the ultimate party data elements in “on behalf of” scenarios. Following the market practice guidelines as outlined on the subsequent pages will enable the industry to realize the benefits of the ISO 20022 standard and eliminate the pain points associated with the incorrect/insufficient data population of ultimate party details.

2.1 Payments/collections on behalf of (POBO/COBO)

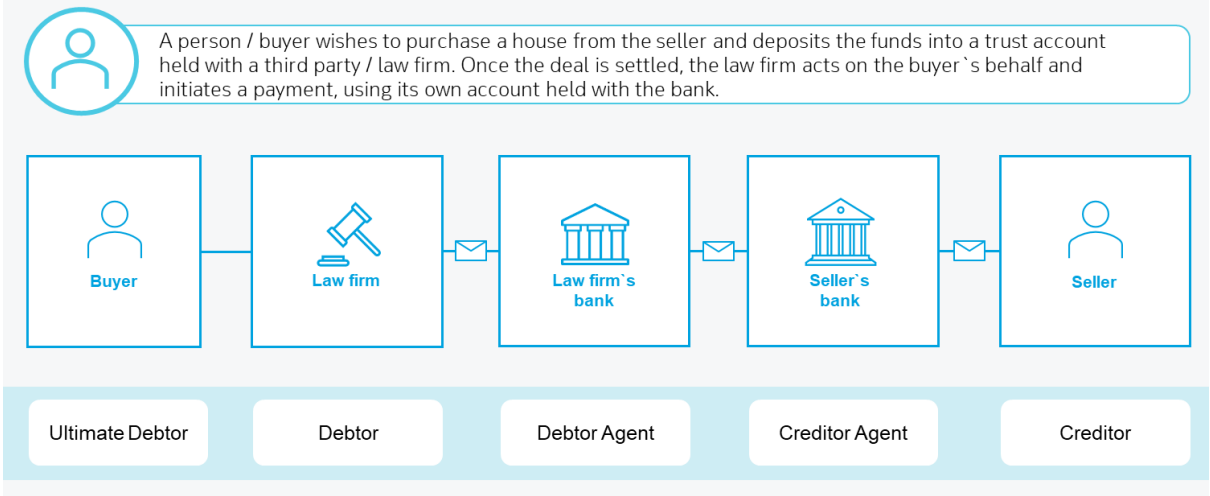
Payments/collections on behalf of (POBO/COBO) are transactions executed by a third party on behalf of the ultimate payment initiator/beneficiary:

- Payments on behalf of (POBO) are third-party payments that are executed on behalf by an entity from its own bank account held with the debtor agent (e.g., trust account held by a law firm in trust of its clients with transactions being executed on their behalf as shown in Figure 2);
- Collections on behalf of (COBO) – also known as “receivables on behalf” of (ROBO) – are third party collections that are received into the entity`s bank account with the creditor agent on behalf of the operating companies (e.g., collection agency scenario, where a firm collects money on behalf of its clients).

Payment transparency standards

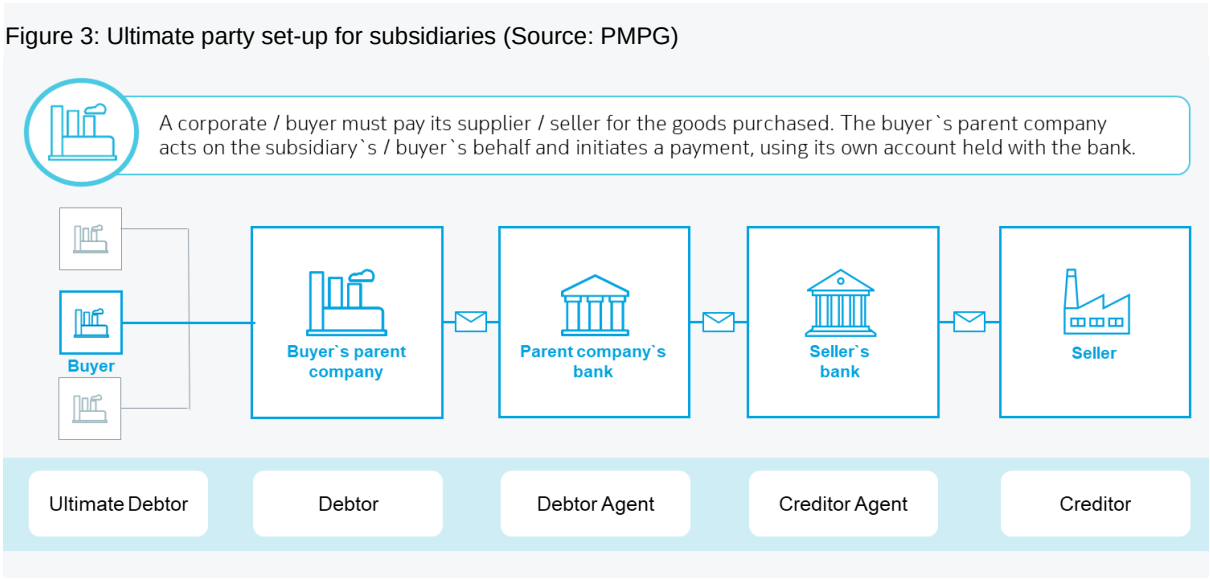
According to the Wolfsberg Group, considering the sensitivity associated with party information, in order to allow corporate entities to make payments on behalf of other parties, these arrangements must be understood by the debtor agent/payment service provider (PSP) to ensure the OBO relationship is permissible under local regulation, e.g., regarding custodial or fiduciary relationships. In the scenario of a law/notary firm or similar legal entity, the transaction initiated by the legal entity from the trust/escrow account is on behalf of its customer, who is the ultimate debtor. The legal entity is not itself a PSP, but it is using its account with the debtor agent PSP to conduct a transaction on behalf of a third party who is not a customer of the debtor agent PSP.

Figure 2: Ultimate party set-up for trust accounts (Source: PMPG)



An “on-behalf-of” set-up is often a means of centralization, standardization and automation of transaction flows of a company through a designated entity, for instance, a payment factory or in-house bank. In such a scenario, a payment factory acts as a correspondent for the operating companies (e.g., subsidiaries) and processes payments/collections from its own bank account on their (e.g., subsidiaries’) behalf as shown in Figure 3, which may significantly reduce the number of accounts to be maintained by the company and streamline its account management.

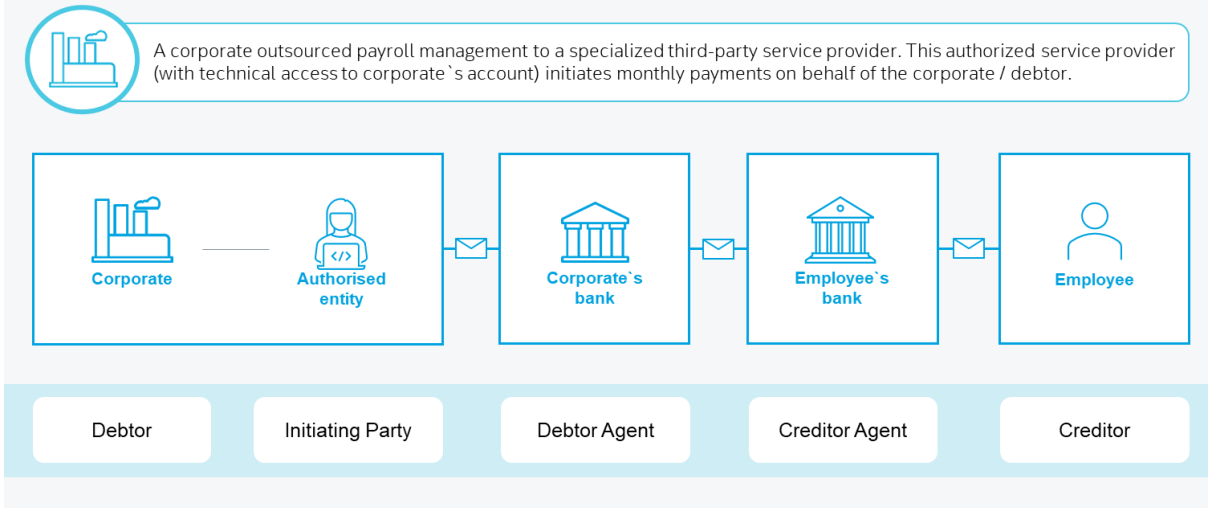
Figure 3: Ultimate party set-up for subsidiaries (Source: PMPG)



Besides the origination/destination of funds at/to a different party, as well as the distinct difference in legal structure of ultimate debtor/ultimate creditor vs. debtor/creditor (ultimate party must be a different legal entity), one of the key characteristics common for POBO/COBO scenarios is that the ultimate debtor/beneficiary of a payment does not hold a bank account with debtor agent/creditor agent – instead, the debtor’s/creditor’s account with the debtor agent/creditor agent is being used.

This, in turn, implies that an entity, which initiates a payment out of a client’s bank account with a debtor agent (with technical control over the account rather than ownership), does not fulfill the ultimate party definition. Such an entity should be identified as an initiating party in a payment message with its client (the account owner) being identified as a debtor as shown in Figure 4.

Figure 4: Initiating party set-up (Source: PMPG)



2.2 Importance of ultimate party identification

To avoid manual intervention, investigations, delays in payment processing and increased costs, the correct population of the payment messages is crucial.

Given that ultimate parties are defined as sensitive payment information, their correct identification and provision in the payment messages is particularly important for anti-financial crime controls. Any non-compliance (for instance, concealing of the ultimate beneficiary details) is subject to regulatory consequences. This is also reflected in the revised Wolfsberg Group Payment Transparency Standards. It is the responsibility of the agent servicing the account of the debtor/creditor to determine if the ultimate party elements are correctly used.

In the correspondent banking space and on the Swift network, Cross-Border Payments & Reporting Plus (CBPRplus) usage guidelines define data requirements for ultimate parties. During the Swift MT-ISO 20022 co-existence phase, it was decided to govern the usage of various ultimate party identifications options (e.g., name, postal address, Business Code Identifier (BIC), Legal Entity Identifier (LEI), date and place of birth, etc.) via textual rules instead of network validation.

This is set to change at the end of the co-existence period when stricter validation for ultimate parties will come into force, mandating the presence of a name and full postal address (Figure 5) in the absence of a structured identifier, e.g., Business Code Identifier (BIC) or the Legal Entity Identifier (LEI) as a potential substitute to the postal address, etc.

This requirement is expected to be further enforced by the ISO 20022 core data model introduced by the BIS Committee on Payments and Market Infrastructures (CPMI). By the end of 2027 at the latest, the payments industry, including payment service providers and payment system operators, are expected to comply with the requirements to identify all financial institutions (FIs), entities and persons involved in a cross-border payment in a standardized and structured way.

Figure 5: Ultimate party identification options (Source: PMPG)

Party	Data element	Sub-element	Comments
Ultimate Debtor Ultimate Creditor	Name	-	Expected to be provided together with Postal Address
	Postal Address	Department	Expected to be provided with Town Name and Country Code as a minimum
		Sub Department	
		Street Name	
		Building Number	
		Building Name	
		Floor	
		Post Box	
		Room	
		Post Code	
		Town Name	
		Town Location Name	
		District Name	
		Country Sub Division	
		Country	
	Identification	Organisation Identification	For instance, Business Identifier Code (BIC) or Legal Entity Identifier (LEI), etc.
		Private Identification	For instance, Date and Place of Birth, Passport Number, etc.
	Country Of Residence	-	Expected to be provided if different from Country

In the meantime, the usage and population of ultimate party data elements will be measured and monitored by the data quality reporting, which is expected to be introduced by Swift in the next years.

Postal address in payment messages

In the absence of a global universal postal address standard and considering the existing various data sources at the payment origin, the industry revised the plan on the decommissioning of the unstructured Postal Addresses in payment messages.

Effective November 2025, ISO 20022 messages used for clearing and settlement of cross-border payments will facilitate the following options:

1) Fully structured postal address as a preferred option.
2) Semi-structured ("hybrid" postal address, also referred to as the "hybrid format", with the minimum of country and town provided in dedicated ISO 20022 data elements.
3) Fully unstructured postal address, which will only be available until November 2026 to facilitate the transition and to allow sufficient lead time for the corporate industry to structure the party address data.

Given the absence of the unstructured postal address data element for ultimate parties in the current usage guidelines and in order to enable option 2) as per the above, the unstructured <Address Line> element is expected to be introduced for ultimate parties in November 2025. For further information, please refer to PMPG market practice guidelines "Structured ordering and beneficiary customer data in payments".

Whilst it is the responsibility of the debtor/creditor to source the data of the ultimate debtor/ultimate creditor (for instance, via Enterprise Resource Planning (ERP), customer system, etc.), the debtor agent/creditor agent is expected to request its clients to always provide full name, address or structured identification of the ultimate parties of the payment and enable the provision of such information in the respective front-end channels. In addition, debtor agents are expected to encourage their clients to adopt the CGI MP[2] pain.001 version 9 payment initiation message given its enhanced interoperability with interbank messages as opposed to the pain.001 version 3.

Furthermore, all agents within a given transaction must ensure that ultimate party information is forwarded unaltered along the payment chain to ensure data integrity and support anti-financial crime processes.

3 Best practices and examples of incorrect message population

Considering the importance of the ultimate party information in payment messages, this section provides guidance to the industry on the correct data provisioning and explores some of the most prominent examples of wrong population of ultimate party information to avoid incorrect usage in future.

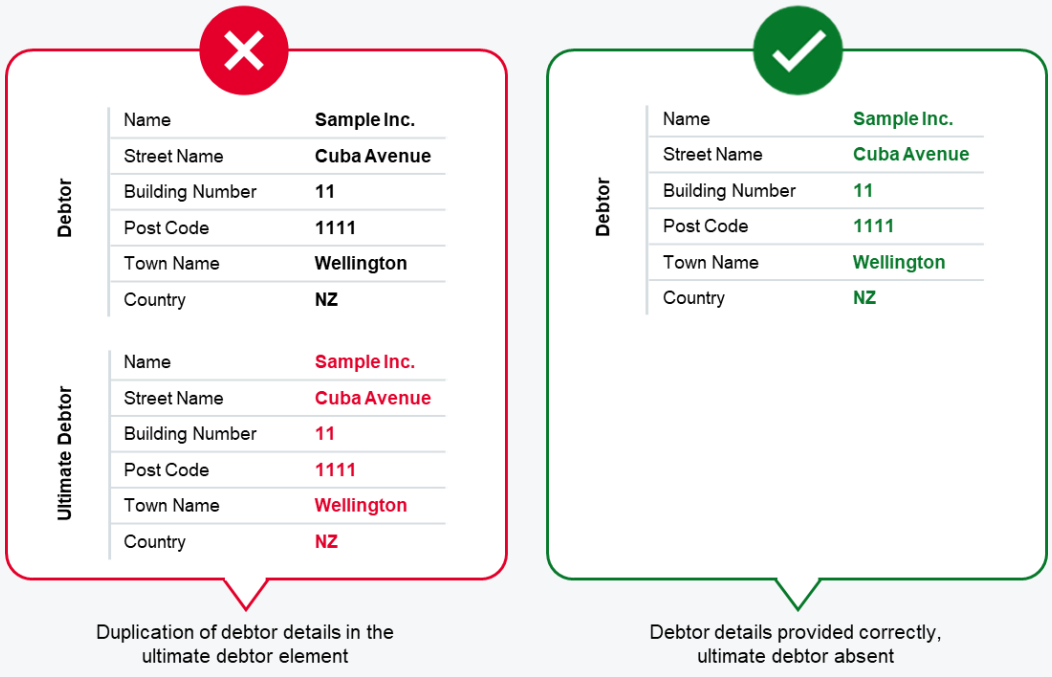
3.1. Duplication of the debtor/creditor details in the ultimate party elements

Ultimate debtor/ultimate creditor is an optional data element in ISO 20022 payment messages, which must only be used if the given payment scenario satisfies conditions of an "on-behalf-of" transaction (as explained in the previous sections). In all other scenarios, this data element must be absent.

[2] Common Global Implementation | Swift

Duplication of the debtor/creditor details in the ultimate party elements is not allowed and is considered an incorrect practice, which is likely to lead to additional effort on the receiver's side and cause payment delays increased costs.

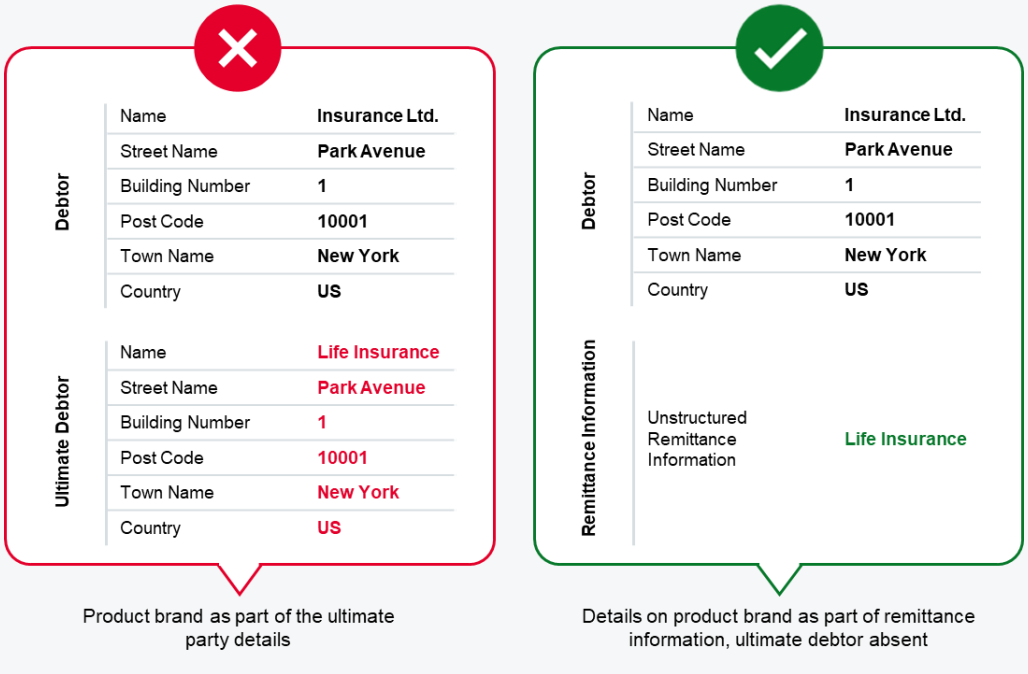
Figure 6: Duplication of the debtor details in the ultimate party elements (Source: PMPG)



3.2. Product name as part of ultimate party details

Ultimate party data elements have been observed to be mistakenly used as a data element to provide additional details on the transaction purpose, for instance, the product name of the purchased goods. Considering that this represents "pollution" of the ultimate party data element, such practice is not permitted – ultimate party data element may only be used in line with the ISO 20022 definition.

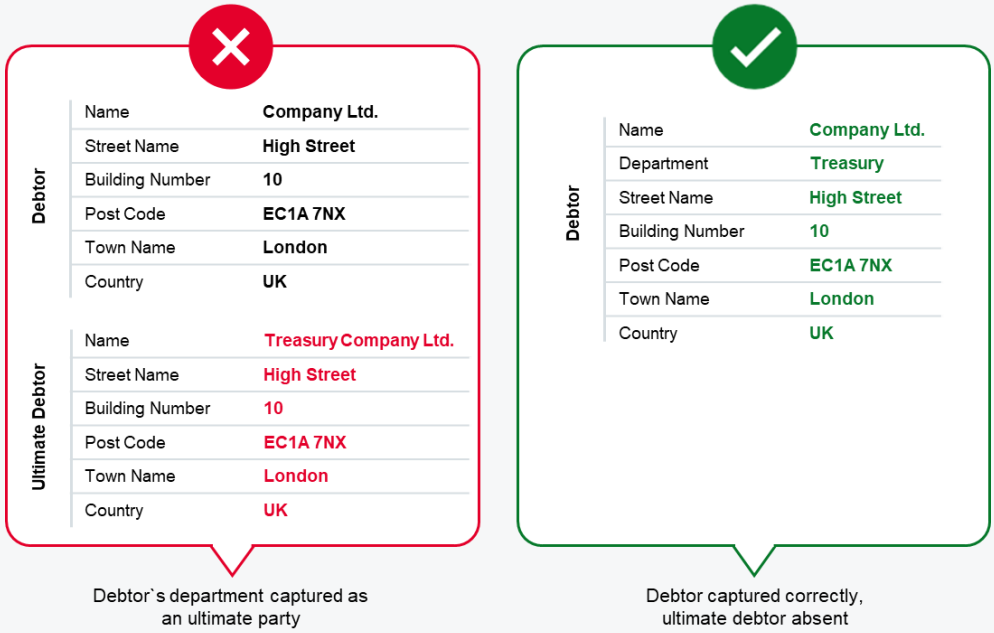
Figure 7: Product name captured as part of ultimate party (Source: PMPG)



3.3 Provision of debtor's department details

As highlighted previously, ultimate party data elements must only be populated in line with ISO 20022 definition. Given that an ultimate party must be a distinct legal entity, different from the debtor/creditor, any incorrect provision of data, such as population of a department of the debtor, "doing business as" or trade names, is considered erroneous usage and may lead to payment delays/increased costs.

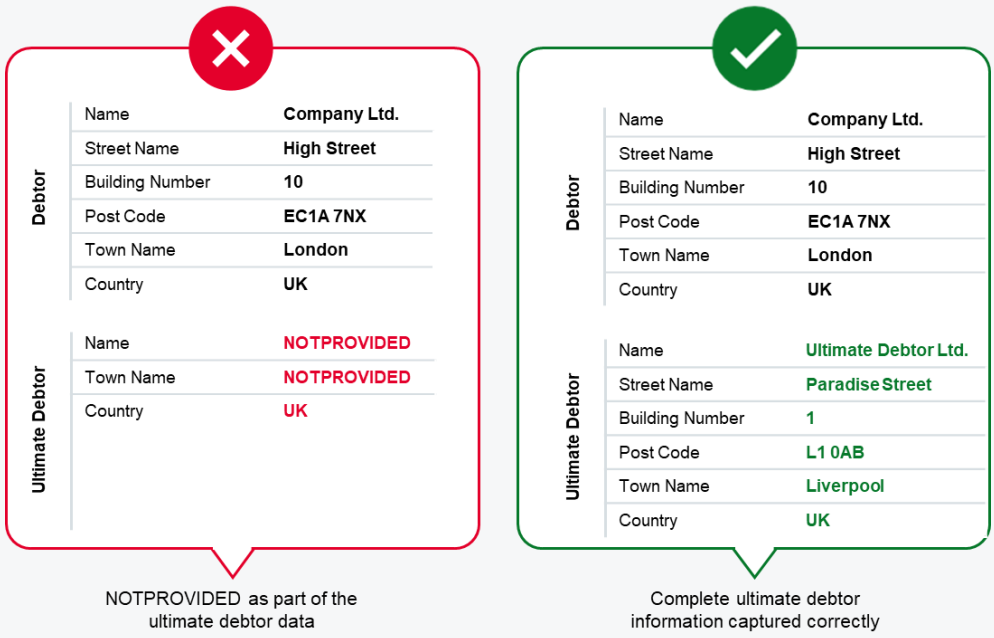
Figure 8: Debtor`s department captured as ultimate debtor (Source: PMPG)



3.4. Provision of ultimate party details as "NOTPROVIDED"

Given the importance of the ultimate party information for anti-financial crime controls, when used, ultimate parties must be populated with meaningful and complete data, such as valid name and postal address, structured identifiers, etc. The population of "NOTPROVIDED" to identify ultimate party should be avoided. In the absence of information for non-mandatory data elements, these should not be present.

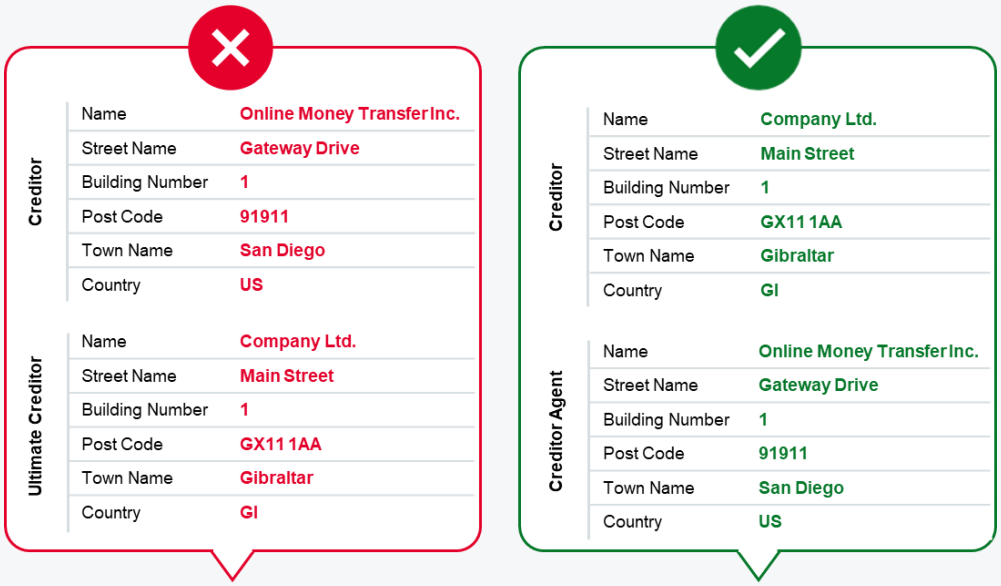
Figure 9: "NOTPROVIDED" as part of data input (Source: PMPG)



3.5. Capturing of payment service providers

The provision of the ultimate party data has been observed to be particularly troublesome with regards to payment scenarios including “new” service providers, for instance, online money transfer companies acting as payment service providers (PSPs).

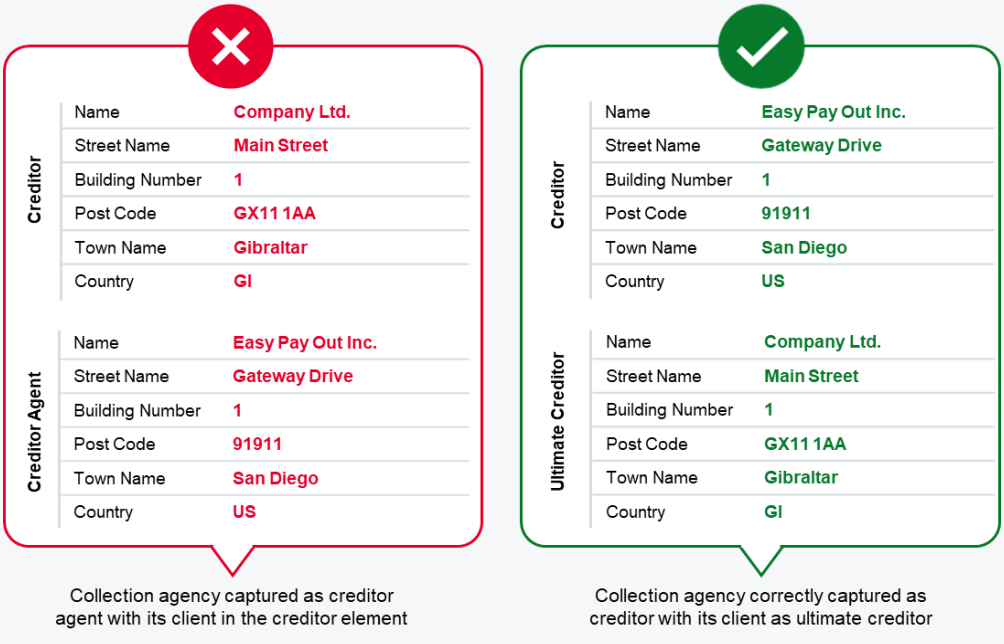
Figure 10: Payment Service Provider as creditor agent (Source: PMPG)



If their capacity as payment service provider, such companies must be identified as an agent (debtor agent/creditor agent), with the client holding an account wallet of the PSP being populated as a debtor/creditor. Given that such a scenario does not satisfy the conditions for an ultimate party set-up, the usage of ultimate party data elements is not permitted.

If, however, a company acts in its capacity as a collection agency (for instance, offering collection services), this is considered a valid scenario for ultimate party population, with the company being captured as the creditor and the underlying merchant being populated as the ultimate creditor.

Figure 11: Collection agency captured as creditor (Source: PMPG)



To contact the PMPG or provide feedback on the content of this paper, please email **info@pmpg.info**

Follow us on LinkedIn