

StoneX

Beyond Message Conversion

Preparing for Swift's November 2026
postal-address requirements

August 2026



For payments operations and transformation leaders at banks and regulated payment providers, with guidance for technology, data, and governance teams.

Introduction: What changes in November 2026

Financial institutions may have completed the headline work of migrating cross-border payment instructions to ISO 20022 and still face a consequential data-readiness problem.

Postal addresses can continue to enter the payment chain as free text through customer records, payment files, proprietary channels, legacy applications, and third-party data, even when the outgoing message is produced in ISO 20022.

From 14 November 2026, fully unstructured postal addresses will no longer be supported in applicable CBPR+ payment messages. Where postal-address information is required or supplied, Town Name and Country must appear in their designated fields at a minimum.¹

After the cutover, institutions may use either a fully structured or hybrid postal address.

The deadline removes one of three currently accepted formats; it does not mandate fully structured output in every case or require every possible address element to be populated.

The operational question is whether an institution can obtain the minimum required data, preserve it across channels and transformations, detect defects before submission, and govern cases that cannot be resolved automatically.

In practice, readiness is more than a message-conversion exercise. It is an end-to-end address-data, channel, validation, exception-management, and governance challenge.

This paper explains the accepted address formats, shows where readiness gaps can arise across the payment chain, and provides a practical framework for assessing and treating exposure.

Structured and hybrid addresses: Both accepted, operationally different

A fully structured postal address uses only the dedicated ISO 20022 postal-address elements. When a postal address is provided, Town Name and Country are required; other available components – such as Street Name, Building Number, Postal Code, Building Name, and Floor – are placed in their corresponding structured elements. The free-form Address Line element is not used.

| Hybrid is not “fully unstructured” under another name.

Format	Required structure	After 14 Nov 2026	Practical implication
Fully structured	Town Name and Country at minimum; available components use designated elements; no Address Line.	Accepted	Strongest basis for machine-readable, granular data.
Fully structured	Town Name and Country structured; additional structured fields permitted; up to two 70-character Address Lines for residual data.	Accepted	Accepted flexibility where complete separation is not reliable.
Fully unstructured	Address supplied only through free-form Address Lines without the minimum structured fields.	Not supported	Source, channel, mapping, or repair changes are required.

Sources: Swift, “Unstructured address data is being removed. Are you ready?”; Payments Market Practice Group, Hybrid Postal Address, Version 1.12, 5 March 2026

A hybrid address also places Town Name and Country in their designated fields. Residual information that cannot be reliably separated may remain in up to two Address Line occurrences of 70 characters each. Additional structured elements may be used, and information already provided in a structured field should not be duplicated in an Address Line.ⁱⁱ

Hybrid accommodates cases in which the minimum fields can be structured but source systems cannot yet separate every remaining component safely. Fully structured data generally offers the strongest basis for automated recognition and downstream processing; hybrid preserves necessary flexibility.

An institution may select different target formats for different sources or channels, provided each output meets the applicable requirements and is supported across the payment route.

The problem begins upstream of Swift

Producing an ISO 20022 message does not prove that the institution possesses payment-ready address data. Required information may originate in customer onboarding records, beneficiary master data, ERP platforms, APIs, host-to-host files, branch systems, or proprietary channels. At each handoff, components can be omitted, combined, duplicated, truncated, or mapped into fields that do not support the required output.

Creditor data creates a particular challenge because it often comes from corporate customers and other payment initiators. A financial institution may control message generation without controlling the quality or structure of the underlying address.

Readiness depends in part on whether customer-facing channels can capture Town Name and Country explicitly, and whether customers can provide those elements consistently.

Translation does not remove that dependency. It can map identifiable source information into a new format; it cannot reliably manufacture a missing country, resolve every ambiguous free-text string, or decide whether an inferred result is sufficiently reliable for payment processing.

Swift similarly notes that translation tools use predefined mapping rules and cannot map free-text information into structured data elements.ⁱⁱⁱ

The appropriate unit of analysis is the full data chain: source record, initiation channel, mapping or transformation, validation, network submission, and exception handling.

The central question is not simply, “Can we send the message?” It is, “Can we identify, validate, and govern the address data needed to move the payment through its intended route?”

How address defects surface

Address defects can surface at different points and should not be described as one universal outcome. A messaging interface applying schema validation may reject an invalid instruction before network submission.

Under CBPR+, a payment containing a fully unstructured address may receive a network-level negative acknowledgement. A payment service provider may reject or delay an instruction, while another defect may be routed into manual repair.^{iv}

Readiness must follow the address from origin through payment processing—not examine the outgoing message in isolation.

These outcomes are possible, not inevitable for every address problem. What happens in practice depends on where the defect is detected, whether reliable data is available for correction, who has authority to repair it, and whether the payment can still meet its processing window.

Swift has stated that it will not provide a contingency mechanism for noncompliant address data because the information must be sourced at origin. Institutions need both preventive controls and a governed response for rejections, repairs, and unresolved cases.^v

A cutover-specific exception requires its own plan

One scenario crosses the deadline itself. A payment instruction accepted before 14 November 2026 may need to be forwarded or reissued over Swift after the cutover.

If the original instruction contains a fully unstructured address, an intermediary processing the subsequent leg may be unable to transmit the address in the same form.

The Payments Market Practice Group's Transitional Cutover Handling guidance describes a strictly temporary, last-resort treatment for qualifying pre-cutover transactions. Where Town Name cannot be reliably identified, the guidance describes use of the standardized value CUTOVER2026. Where Country is unavailable, it describes last-resort derivation from the Creditor Agent BIC, while cautioning that the resulting country may not reflect the party's actual location. PMPG states that this treatment applies only to transactions initiated before the cutover, must not be used for newly initiated payments, and should be limited to a maximum of three months after go-live.^{vi}

This is not a Swift contingency mechanism or a general substitute for missing address data. Defaulted or derived values require explicit governance, traceability and institutional approval because they may not represent authoritative party information.

A five-lens readiness diagnostic

A useful assessment should follow the address from origin through payment processing rather than examine the outgoing message in isolation. Five lenses can reveal where exposure exists, who owns it, and what treatment is required.

Lens 1: Source data and ownership

Core question: Do we possess the required information, and who is accountable for its quality?

Review: Inventory sources for debtor, creditor, ultimate-party, and relevant agent addresses. Measure fully unstructured records and missing Town Name or Country, identify third-party dependencies, and assign business and data owners.

Outcome: A quantified source-data baseline with accountable owners and identified third-party dependencies.

Lens 2: Channel capture and client readiness

Core question: Can every relevant channel collect and transmit the minimum structured information?

Review: Examine applications, customer files, APIs, host-to-host connections, branches, and legacy formats. Identify affected clients and define communication, specification changes, and migration support.

Outcome: A channel-by-channel view of required changes, affected clients, and readiness actions.

Lens 3: Mapping, transformation, and validation

Core question: Does information reach the correct output fields without loss, duplication, or misinterpretation?

Review: Trace representative addresses end to end, confirm how structured and hybrid outputs are produced, and distinguish deterministic mapping from parsing or inference.

Outcome: Evidence that mappings preserve address components and a defined treatment for flows that require parsing or inference.

Lens 4: Exceptions and repair

Core question: What happens when an address is incomplete, ambiguous, or cannot be structured confidently?

Review: Define exception triggers, confidence thresholds, manual-review authority, audit requirements, escalation paths, service expectations, and likely volumes. Include cutover-specific rules for payments initiated before the deadline but retransmitted afterward, including eligibility, permitted default or derivation logic, expiration dates, audit evidence, and approval authority.

Outcome: A governed operating model for unresolved cases, including ownership, controls, capacity, and escalation.

Lens 5: Testing and governance

Core question: Can the institution demonstrate readiness across actual routes and sustain it after cutover?

Review: Test representative messages, channels, clients, counterparties, and exception scenarios. Assign cross-functional ownership and monitor format mix, failures, repairs, and recurring source defects.

Outcome: End-to-end readiness evidence, accountable governance, and measures for sustained control.

The result should be more than a technical defect list: it should identify priority exposures, affected flows, accountable owners, and an explicit treatment decision for each material gap.

Choose a layered remediation path, not a single fix

No single remediation method will suit every source or flow. Institutions will generally need a combination of preventive, corrective, automated, and exception-based controls.

Correct data at the source. This is the strongest long-term response where the institution controls the data, but it cannot supply genuinely missing information without an authoritative source.

Improve channel capture and validation. Prevents new defects by requiring minimum structured fields. It may require application changes, customer communication, revised specifications, and consistent enforcement.

Select the appropriate output format. Use fully structured output when components map reliably; use hybrid when Town Name and Country can be structured but residual information cannot be separated safely.

Apply bounded structuring or inference. This may extract required elements from legacy inputs, but it requires confidence criteria, validation, documented limits, and a route for uncertain results.

Govern manual repair. Manual repair can address ambiguous or incomplete cases, but it requires clear authority, traceability, escalation, capacity planning, and treatment before cut-off.

Embed controls through APIs or middleware. APIs or middleware can incorporate validation and transformation into existing flows, subject to supported messages, architecture, security, volumes, and operational support.

The objective is a layered response: correct what can be corrected at source, prevent recurrence through channel controls, automate cases that can be handled reliably, and govern the remainder.

From assessment to readiness

Selecting the appropriate controls is only one part of readiness; institutions should also sequence, assign, test, and monitor the work.

The diagnostic becomes useful when it produces an accountable readiness program. A practical sequence is to:

Baseline exposure. Measure the three address formats and connect the results to sources, channels, messages, clients, and owners.

Prioritize material flows. Rank exposures by volume, client impact, data quality, channel complexity, operational risk, and exception demand.

Define target treatments. Decide where fully structured or hybrid output, source cleanup, channel changes, inference, integration, or repair belong.

Establish exception governance. Set validation criteria, thresholds, queues, owners, escalation paths, audit requirements, and cut-off procedures.

Test end to end. Exercise representative data, channels, mappings, validations, counterparties, and operational handoffs.

Monitor and improve. Track format mix, validation failures, negative acknowledgements, repair volumes, aging, and recurring defects.

Where StoneX can contribute

StoneX Technology Services can help banks and regulated payment providers examine address-data readiness before selecting a remediation path. StoneX can begin by analyzing client-provided messages, source records, or address data within an agreed scope.

StoneX Technology Services has served as a trusted Swift-certified Service Bureau^{vii}, member, partner, and provider of Swift services since 2002, supporting financial institutions across Swift connectivity, managed operations, reporting, analytics, and financial messaging. StoneX Messaging Hub, version 3, is also listed in Swift's Postal Address Registered Payment Applications directory, based on StoneX's self-attestation that the application can convert unstructured postal address data into fully structured or hybrid format.^{viii}

Assess exposure

StoneX can analyze the supplied data to identify fully unstructured, incomplete, or potentially problematic address records. Depending on scope, StoneX may provide dashboards, record-level findings, exposure summaries, and confidence scores. These findings can help the institution identify concentrations of exposure and set remediation priorities.

Support targeted remediation

Where agreed, StoneX can assist with one-time cleanup or address-structuring activities. The work is bounded by the information available and the institution's rules: it cannot create authoritative data that is absent or determine whether an inferred result should be accepted.

Support address structuring and exception workflows

StoneX offers an API-first product, with accompanying services based on implementation scope, that uses Swift's NLP-based AI address-structuring model^{ix} to infer Town Name and Country from unstructured address content. The product supports Swift-standard payment formats within the agreed technical scope and provides confidence scores for the inferred Town Name and Country. Clients can establish separate confidence thresholds for each field and configure how below-threshold results are handled—for example, by rejecting the message, withholding automated structuring, issuing a notification, or routing the record for review. The institution remains responsible for choosing thresholds, correcting or approving uncertain records, and authorizing payment release.

Support transitional cutover handling

StoneX can support PMPG-aligned exception rules for payments crossing the November 2026 cutover. These include a client-configured default Town Name and optional country-derivation logic for debtor and creditor addresses when the required information is not available directly in the postal address.

The institution chooses whether to apply the derivation logic. The institution remains responsible for defining eligible scenarios, approving default or derived values, limiting their use, and determining whether the resulting instruction should proceed.

A default or derived value can support controlled exception processing, but it does not become authoritative address data merely because it passes message validation.

Preserve institutional accountability

StoneX's role is advisory and supportive. The institution retains accountability for source data, business rules, customer remediation, governance, final testing approval, and compliance decisions. StoneX does not guarantee compliance or payment acceptance.

Conclusion: Readiness begins with the address-data chain

From 14 November 2026, fully structured and hybrid postal addresses remain accepted in applicable CBPR+ payment messages; fully unstructured addresses do not.

The practical task is broader than message conversion: institutions should examine where address data originates, whether channels capture the minimum structured elements, how mappings preserve them, how exceptions are treated, how readiness is tested, and who owns the controls.

Five questions can help readiness leaders focus the remaining work:

- Where do fully unstructured addresses still enter our payment chain?
- Can every relevant channel capture Town Name and Country explicitly?
- Where could mappings or transformations lose, duplicate, or distort address components?
- How will incomplete or ambiguous records be repaired and governed?
- Can we demonstrate readiness across representative clients, channels, routes, and exception scenarios?

Sources and further reading

[Unstructured address data is being removed. Are you ready?](#)

[A brief introduction to the Postal Address field](#)

[Hybrid Postal Address, Version 1.12](#)

[Swift, "The Swift AI Address Structuring Model"](#)

[Swift payment solutions by StoneX](#)

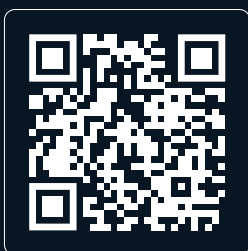
Annex: Sources

- i [Swift, "Unstructured address data is being removed. Are you ready?"](#)
- ii [Payments Market Practice Group, Hybrid Postal Address, Version 1.12, 5 March 2026](#)
- iii [Swift, "A brief introduction to the Postal Address field."](#)
- iv [Swift, "ISO 20022 in bytes for payments: Call-to-action for November 2026."](#)
- v [Swift, "ISO 20022 milestone for November 2026: Unstructured addresses to be removed."](#)
- vi [Payments Market Practice Group, Hybrid Postal Address, Version 1.12, 5 March 2026, pp. 42–45.](#)
- vii [Swift, "Service Bureau Directory."](#)
- viii [Swift, "Postal Address Registered Payment Applications," last updated 22 July 2026.](#)
- ix [Swift, "ISO 20022: The Swift AI Address Structuring Model."](#)

Discuss your readiness

Contact StoneX Technology Services at sts.info@stonex.com to discuss your address data, potential exposure, and an appropriate remediation path.

For more information about StoneX Technology Services, scan the QR code.



The StoneX Group Inc. (the "Company") group of companies provides financial services worldwide through its subsidiaries, including physical commodities, securities, exchange-traded and over-the-counter derivatives, risk management, global payments and foreign exchange products in accordance with applicable law in the jurisdictions where services are provided. StoneX Payment Services Ltd. is a wholly owned subsidiary of StoneX Group Inc. Incorporated in the State of Washington, U.S.A., Washington Corporation (UBI 603 514 004). Authorized and regulated by Money Service Business Multi-State Protocol on NMLS [NMLS:1394445] Licensing and Regulatory Information United States: StoneX Payment Services Ltd. (U.S.A.); Washington Corporation (UBI 603 514 004); Florida HQ (F19000000068); FinCEN Registration as an MSB (31000225191175); Global Markets Entity Identifier (GMEI) (543008RP59ZQ3UQ1882); NMLS Registration (1394445); FINTRAC Registration as an MSB (MSB registration no. M22868358); Revenu Québec Registration as an MSB (MSB license no. 15540). Multiple states use the NMLS ID number (1394445) as StoneX Payment Services Ltd.'s money transmitter license number. This number, as well as any state-specific licensing numbers, are included below for all states in which StoneX Payment Services Ltd. is licensed as a money transmitter: Alabama (MT 811), Alaska (AKMT-016908), Arkansas (129564), Arizona (MT-1000854), California (MT 2653), Colorado (500262), Connecticut (MT-1394445), District of Columbia (MTR1394445), Florida (FT230000308), Georgia (65171), Idaho (MTL-240), Illinois (MT 0000338), Iowa (2019-0003), Kansas (MT.0000148), Kentucky (SC700740), Louisiana (NMLS 1394445), Maine (NMLS 1394445), Maryland (NMLS 1394445), Michigan (MT0022015), Minnesota (MN-MT-1394445), Missouri (MO-20-8525), Nebraska (NMLS 1394445), Nevada (MT11210), New Hampshire (22926-MT), New Jersey (1903874), New Mexico (NMLS 1394445), North Dakota (MT103229), Ohio (OHMT159), Oklahoma (NMLS 1394445), Oregon (30224), Pennsylvania (58690), Rhode Island (20234617CT), South Carolina (NMLS 1394445), South Dakota (MT.2142), Tennessee (NMLS 1394445), Texas (3179), Utah (178), Vermont (MT-1394445), Washington (550-MT-116463), West Virginia (WVMT-1394445), Wyoming (7278). 2026 © StoneX Financial GmbH ("SFG") is a wholly owned subsidiary of StoneX Group Inc. entered in the Frankfurt am Main Commercial Register, HRB 101212, authorized to perform payment service in accordance with § 1 (1) s. 2 No. 6 German Payment Act (ZAG) and regulated by the Federal Financial Supervisory Authority and the German Federal Bank (BaFin-ID: 10141964). 2026 © StoneX Financial Ltd ("SFL") is a wholly owned subsidiary of StoneX Group Inc. All rights reserved. SFL is registered in England and

Wales, company no. 5616586. SFL is authorised and regulated by the Financial Conduct Authority (registration number FRN:446717) to provide to professional and eligible customers including: arrangement, execution and, where required, clearing derivative transactions in exchange traded futures and options. SFL is also authorised to engage in the arrangement and execution of transactions in certain OTC products, certain securities trading, precious metals trading and payment services to eligible customers. SFL is authorised & regulated by the Financial Conduct Authority under the Payment Services Regulations 2017 for the provision of payment services. SFL is a category 1 ring-dealing member of the London Metal Exchange. In addition SFL also engages in other physically delivered commodities business and other general business activities which are unregulated and not required to be authorised by the Financial Conduct Authority. StoneX Financial Pte Ltd (Co. Reg. No. 201130598R) ("SFP") is regulated by the Monetary Authority of Singapore and is a Capital Markets Service Licensee (for dealing in capital market products), an Exempt Financial Adviser (for advising on investment products and issuing or promulgating analyses/reports on investment products) and a Major Payment Institution (for cross-border money transfer service). This document and the information herein is provided confidentially for information purposes only to the recipient and shall not be deemed to be an offer for the sale or purchase of any financial services product transaction or advice. Trading swaps and over-the-counter derivatives, exchange-traded derivatives and options and securities involves substantial risk and is not suitable for all investors. The information herein is not a recommendation to trade nor investment research or an offer to buy or sell any derivative or security. It does not take into account your particular investment objectives, financial situation or needs and does not create a binding obligation on any of the StoneX group of companies to enter into any transaction with you. You are advised to perform an independent investigation of any transaction to determine whether any transaction is suitable for you. This information is provided on an 'as-is' basis and may contain statements and opinions of any StoneX entity as well as excerpts and/or information from public sources and third parties and no warranty, whether express or implied, is given as to its completeness or accuracy. Each StoneX entity (on its behalf and on behalf of its group, directors, employees and agents) disclaims any and all liability as well as any third party claim that may arise from the accuracy and completeness of the information detailed herein, as well as the use of or reliance on this information by the recipient, any member of its group or any third party.