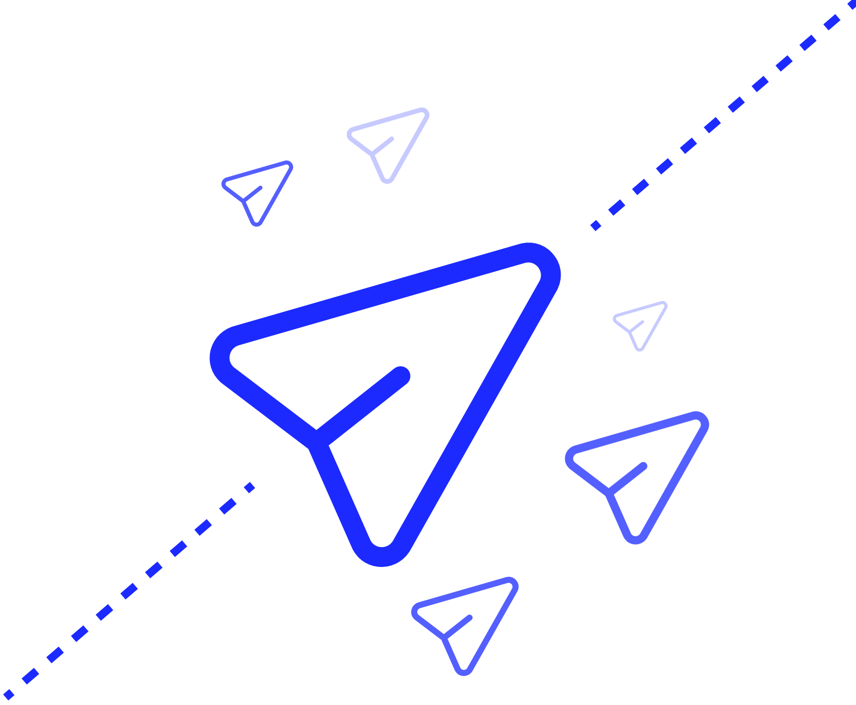
VerbaPulse

Pre-Send Field Guide

Recognising and reducing language risk in financial-services communications, before it leaves the building.

verbapulse.com

VerbaPulse



Written for compliance, MLRO, and risk teams, and for the front-office managers they equip. Use it as a desk reference, a training aid, or the basis of a communications wording standard.

Part 1

Why the message is the control gap

Most communication risk in a financial-services firm is not created in a policy, a training room, or a surveillance queue. It is created in a draft, a few seconds before Send, by someone who is helpful, busy, and moving fast. Policy sits above the message. Surveillance sits after it. The drafting moment itself, where the wording is actually chosen, has almost no control around it.

Regulators have moved to that level. Off-channel communication fines, market-abuse cases built on a single message, and financial-promotion scrutiny under Consumer Duty all turn on what one person wrote in one line. The programmes at those firms were real. The exposure was the individual sentence.

This guide is about the skill that closes the gap: reading your own draft the way a regulator, an auditor, or opposing counsel would read it two years later, and catching the wording while it is still a draft. It covers the six patterns where language most often creates regulatory exposure in financial services, the reasoning behind each, and how to recognise and neutralise them.

The last section is a toolkit you can adopt directly: a pre-send checklist, a red-flag phrase reference, a front-office wording standard, and a short guide to embedding the habit. Nothing here depends on any particular product. The point is the judgement, which travels with the reader.

Part 2

The six patterns, and how to read them

Each pattern below follows the same shape: what it is, the rule behind it, the tell that lets you spot it in a draft, why a well-meaning person writes it anyway, and the principle for fixing it. The examples illustrate the principle; they are not a script.

Part 2

The six patterns, and how to read them

1 Competition and antitrust

What it is.

Coordinating with, or exchanging competitively sensitive information with, a competitor, usually inside what feels like ordinary industry contact.

The rule.

EU and UK competition law (Article 101 TFEU; Chapter I of the Competition Act 1998). Agreements or concerted practices that fix prices, share markets, or exchange future pricing and strategy are among the most serious infringements, with fines up to 10% of global turnover and personal consequences. Intent is not required; the object or effect is enough.

The tell.

Language that coordinates instead of competes. First person plural about pricing ("let's both hold", "neither of us"), forward-looking commercial information ("where you're landing on fees", "our planned increases"), and reassurance against competing ("no point in a price war"). It surfaces at trade fairs, in associations, and on benchmarking calls.

Why it hides.

It reads as courtesy or common sense between people who know each other. Nobody feels like they are running a cartel; they feel collegial, or like they are avoiding a mutually destructive fight.

The fix

There is usually no compliant rewrite. You cannot soften a coordination, so you remove it and keep only genuinely public or historic content. If information sharing has a legitimate purpose, it must be aggregated, historic, and run through a lawful gateway, never swapped in an email.

Risky: Let's both hold our list prices this quarter and not undercut each other at the big accounts.
Recommended action: Remove the coordinating content. There is no compliant version of a pricing arrangement with a competitor.

Risky: Before the next tender, it would help to know where you're landing on fees.
Recommended action: Remove it. Seeking a competitor's forward-looking pricing is itself the risk.

Part 2

The six patterns, and how to read them

2 Market abuse and inside information

What it is.

Sharing material non-public information, disclosing it selectively, or encouraging someone to deal on it.

The rule.

The Market Abuse Regulation (MAR, EU 596/2014, retained in the UK). Unlawful disclosure of inside information and encouraging dealing carry civil and criminal liability, and apply to anyone who holds the information, not only insiders by title.

The tell.

A time or secrecy marker attached to price-sensitive facts. "Before it's announced", "still under embargo", "between us", followed by something that would move a price (a downgrade, a deal, a result, a dividend change), and often a nudge to act ("you may want to move before Friday").

Why it hides.

It feels like being helpful to a client or a colleague, or like normal deal chatter. The line between market colour and inside information is genuinely hard to see in the moment.

The fix

Remove the non-public fact; do not paraphrase it into something softer. Never pair information with a suggestion to trade. Once it is public and the recommendation is properly produced and recorded, it can go through the normal channel. If in doubt, it does not go in an email at all.

Risky: Just between us, the fund is being downgraded before it's announced,
so you may want to move your position.
Recommended action: Remove both the non-public disclosure and the suggestion to trade.

Part 2

The six patterns, and how to read them

3 Financial promotions and performance claims

What it is.

Any communication that promotes a product or service, or describes performance, in a way that could mislead.

The rule.

MiFID II Article 24 and COBS 4: information to clients must be fair, clear and not misleading. Under Consumer Duty it must also support good outcomes and avoid foreseeable harm. Performance cannot be presented as guaranteed, risk cannot be downplayed, and the prominent impression is what counts, more than the small print.

The tell.

Forward-looking certainty and asymmetry. "Will deliver", "you can expect", "guaranteed", "no downside", superlatives such as "best-in-class", and any number offered as a promise. Risk mentioned faintly, or not at all.

Why it hides.

Confidence sells, and a relationship manager wants to reassure.
The writer believes the number, so it does not feel like a claim.

The fix

Convert promises into objectives and restore balance. Use "aims to", "is designed to", or "targets" rather than "will", and state the risk alongside the return at similar prominence. Never guarantee an outcome the firm does not control.

Risky: This strategy will deliver strong double-digit returns with very little downside.
Better: This strategy aims to achieve strong double-digit returns while managing downside risk.

Risky: You can expect around 12% a year, and it won't lose money.
Better: The strategy targets long-term growth. Returns will vary and capital is at risk.

Part 2

The six patterns, and how to read them

4 AML and tipping-off

What it is.

Telling the subject, or a third party, that a suspicious-activity report has been made or that a money-laundering review is under way.

The rule.

In the UK, section 333A of the Proceeds of Crime Act 2002 makes tipping-off a criminal offence, and equivalent duties run through EU AML regimes. The offence is committed even when the disclosure is casual and well-meant.

The tell.

Explaining a delay or a block by naming the real reason. "Flagged for a money-laundering review", "our financial crime team is investigating your account", "we filed a report". The tell is any wording that reveals the review, or the report, to the person under it.

Why it hides.

The writer is trying to be transparent and helpful, which is exactly the instinct that creates the offence.

The fix

Give a neutral, true, non-specific reason, and never reference a report, an investigation, or financial crime to the subject.

Risky: We can’t process your transfer because it’s been flagged for a money-laundering review.
Better: We can’t process your transfer right now because it is going through additional compliance checks.

Part 2

The six patterns, and how to read them

5 Client confidentiality and data

What it is.

Sharing more client information than the recipient needs, or disclosing confidential relationships, holdings, or identifiers.

The rule.

Contractual and professional confidentiality duties, together with GDPR: personal data must be adequate, relevant, and limited to what is necessary (data minimisation, Article 5). Over-disclosure is both a confidentiality breach and a data-protection one.

The tell.

Full identifiers where a summary would do (account numbers, whole portfolios, client names paired with sensitive facts), and secrecy framing ("keep this to yourself") that shows the writer already senses it is sensitive.

Why it hides.

Attaching everything is faster and feels thorough. The writer is giving context, without thinking about minimisation.

The fix

Share the minimum the recipient needs to act. Summarise rather than attach raw data, strip identifiers, and ask whether this recipient needs this detail at all. Need-to-know is the default; full disclosure is the exception.

Risky: I'm attaching the client's full portfolio and account numbers so you have the background.
Better: I'm attaching a summary of the client's portfolio so you have the background.

Part 2

The six patterns, and how to read them

6 Binding commitments and over-promising

What it is.

Turning an email into a contractual commitment, or promising an outcome or timeline the firm cannot control.

The rule.

Under English and most EU law a binding contract can form through an email exchange, with no signed document, if the elements are present. Words such as "binding confirmation" and "we guarantee", paired with specific terms, can convert a discussion into an enforceable obligation.

The tell.

Commitment language and personal guarantees. "Please treat this as a binding confirmation", "we guarantee", "you have my word", "consider this a formal record", paired with a rate, a term, exclusivity, or a date.

Why it hides.

The writer wants to reassure or to close, and treats confirming as good service. The legal weight of the words is invisible to them.

The fix

Remove the committing force, not only the adjective. Use "subject to a signed agreement" and "our current expectation" in place of "binding confirmation", and state intent in place of a guarantee. Anything genuinely binding goes through a contract, not an inbox.

Risky: Please treat this email as our binding confirmation that we guarantee the 0.5% fee for five years.
Better: This summarises the 0.5% fee we discussed for five years, subject to our final signed agreement.

Risky: You have my word we'll get you authorised in eight weeks, guaranteed.
Better: We're aiming for authorisation within about eight weeks. Timelines depend on the regulator.

Part 3

What enforcement actually looks like

The patterns in Part 2 are not theoretical, and they are not historical. Every case below is from 2024 to 2026 and is public record. Each turned on an ordinary working moment: a message on the wrong channel, a check that was not run, a word to a friend, a CC field. They are summarised here for the lesson they carry, not to alarm. Details are simplified; the sources are given so you can read the originals.

Part 3

What enforcement actually looks like

The off-channel sweep reaches its fourth year

U.S. SEC I January 2025 I $63 million across 12 firms, on top of more than $2 billion since 2021

On 13 January 2025 the SEC settled with twelve more investment advisers and broker-dealers over business messages sent on personal devices and unmonitored apps, adding $63 million to a sweep that has now charged well over a hundred firms and collected more than $2 billion since December 2021. The penalties in this round ran from $4 million to $12 million per firm; one firm that had self-reported was capped at $600,000. The conduct being punished was not fraud or manipulation. It was where and how people wrote, and whether the record could be produced when the regulator asked.

The lesson.
Four years in, the message itself remains the regulatory object. Firms keep paying because the control that failed was the moment of writing, in channels the compliance function could not see.

Source: SEC press release, 13 January 2025; SEC and CFTC enforcement announcements 2021 to 2025 (sec.gov).

The information that was in the file all along

UK FCA I July 2025 I £42 million, Barclays

In July 2025 the FCA fined Barclays a combined £42 million across two financial-crime cases. In one, the bank opened a client-money account for WealthTek without a basic check of the Financial Services Register, which would have shown the firm was not permitted to hold client money; £34 million of client funds went into the account. In the other, it banked Stunt & Co, which received £46.8 million in a year from a business later prosecuted for money laundering, and did not act on the warning signs until a competitor's prosecution became public.

The lesson.
The failures were not about a lack of information. The information existed and was reachable. Nobody checked at the moment that mattered, before the account was opened and the relationship began.

Source: FCA press release, "FCA fines Barclays £42 million for poor handling of financial crime risks", July 2025 (fca.org.uk).

Part 3

What enforcement actually looks like

The interim CFO and the trader

UK FCA I February 2026 I £108,731 combined, two individuals

In February 2026 the FCA fined the interim chief financial officer of Bidstack, an AIM-quoted advertising-technology company, and a trader a combined £108,731. The CFO held confidential information about a significant deal with a video-game publisher, disclosed it to the trader, and helped open a trading account in the trader's name; together they bought 1.3 million shares before the announcement. The share price rose more than 125% on the news. The trader's profit was roughly £9,000. Both were fined and named.

The lesson.
Unlawful disclosure and insider dealing are prosecuted at any scale. A £9,000 gain produced six-figure penalties, public findings, and the end of a career. The disclosure to a friend is the offence, whatever the format.

Source: FCA press release, "FCA fines two individuals a combined £108,731 for insider dealing", 10 February 2026 (fca.org.uk).

The CC field, again

UK ICO I April 2024 I £7,500 and a reprimand, Central YMCA

A programme coordinator at Central YMCA in London emailed participants of an exercise programme for people living with HIV using CC instead of BCC. Two hundred and sixty-four addresses were exposed to every recipient; 166 individuals could be identified or potentially identified, so that their likely HIV status could be inferred. The ICO originally proposed a £300,000 fine, reduced under its public-sector approach, and issued a reprimand alongside it. The Commissioner used the case to warn that this exact error keeps recurring across the sector.

The lesson.
One habitual keystroke, one field, one email. Data minimisation and recipient mechanics are pre-send questions, and the regulator has said, in terms, that it will keep penalising them.

Source: ICO enforcement action and Commissioner's statement, April 2024 (ico.org.uk).

Part 3

What enforcement actually looks like

Fifty-four thousand accounts that should not have been opened

UK FCA I October 2024 I £29 million, Starling Bank

The FCA fined Starling Bank £28.96 million for financial-crime failings, including a sanctions-screening system that for years checked only a fraction of the relevant lists, and the repeated breach of a requirement not to open accounts for high-risk customers: more than 54,000 accounts were opened for around 49,000 such customers over two years. The failings were systemic, at a fast-growing bank whose controls did not keep pace with its onboarding.

The lesson.
Controls have to run at the moment of the decision, not be reconciled afterwards. When onboarding, screening, or drafting outpaces the check, the record fills with decisions nobody stopped.

Source: FCA press release, "FCA fines Starling Bank £29m for failings in their financial crime systems and controls", October 2024 (fca.org.uk).

Three threads run through all five, and all of them are recent. The exposure was created in an ordinary working moment: a message, an account opening, a CC field, a word to a friend.

The record was read afterwards, cold, by someone reconstructing what happened from the trail alone. And in every case the control that failed was not a policy, which existed, but the moment of action, which nothing guarded.

Part 4

The toolkit

Adopt these directly. The checklist and the wording standard can go into a policy or a one-page card for client-facing staff, and the red-flag reference works as a desk aid.

Part 4
The toolkit

A The pre-send checklist

Ten questions to run over a draft before Send.
If any answer is yes, stop and reword or remove.

1. Does any sentence make a promise, guarantee, or commitment the firm cannot fully control?
2. Is a return or outcome presented as certain, or is the risk played down?
3. Does it share anything that is not yet public and could move a price or a decision?
4. Does it coordinate with, or seek forward-looking information from, a competitor?
5. Does it reveal a compliance, AML, or financial-crime review to the person under it?
6. Does it share more client data or identifiers than this recipient actually needs?
7. Read cold in two years, would any line look like coordination, a promise, inside information, or a contract?
8. Is confidential or NDA-covered information going to someone outside the need-to-know circle?
9. Does the prominent impression meet the fair, clear and not misleading standard?
10. If anything here is genuinely binding, should it sit in a contract instead of an email?

Part 4

The toolkit

B The red-flag phrase reference

Common wording that should make a writer pause, and the principle that applies.

If the draft says	The principle
"we guarantee" / "you can expect" / "will deliver"	State an objective rather than a promise, and keep the risk visible.
"no downside" / "risk-free" / "can't lose"	Keep risk in the picture and describe how it is managed.
"binding confirmation" / "a formal record"	Nothing binds until it is signed. Use "subject to a signed agreement".
"you have my word" / "I promise"	Replace a personal guarantee with the firm's position.
"just between us" / "keep this to yourself"	A secrecy marker is a warning. Check for inside information or confidentiality first.
"before it's public" / "under embargo"	Do not disclose non-public, price-sensitive facts. Wait for the announcement.
"you may want to move" / "act before Friday"	Never pair information with a suggestion to trade.
"let's both hold" / "neither of us should undercut"	Remove it. You cannot coordinate pricing with a competitor.
"where are you landing on price" / "your planned increases"	Do not seek or share forward-looking competitor information.
"flagged for a money-laundering review" / "under investigation"	Give a neutral reason. Never reveal a review or a report to the subject.
"attaching the full portfolio" / "account numbers"	Share the minimum needed. Summarise and strip identifiers.
"as agreed, the rate is X for Y years"	If it is meant to bind, put it in a contract. Otherwise mark it as a discussion.

Part 4

The toolkit

C A front-office wording standard

Ten house rules you can drop into a communications policy or a one-page brief for client-facing teams.

1. We describe objectives rather than guarantees. Returns are never certain, and risk is always stated.
2. We keep risk and return at equal prominence.
3. We do not confirm anything as binding by email. Binding terms live in a signed agreement.
4. We replace personal guarantees with the firm's position.
5. We do not share non-public, price-sensitive information, and we never suggest trading on it.
6. We do not coordinate pricing or exchange forward-looking commercial information with competitors.
7. We give neutral reasons for delays. We never tell a customer their transaction is under a financial-crime review.
8. We share the minimum client data a recipient needs, and we summarise rather than attach raw detail.
9. We treat "just between us" as a prompt to stop and check.
10. When in doubt, we ask compliance before we send.

Part 4

The toolkit

D Embedding the habit

Run a short session per team using their own real, redacted emails, rather than one slide deck for everyone. People learn from their own wording.

Teach three habits: read the draft as a stranger would in two years; treat absolute words as a stop sign; when a line feels like a commitment, make it subject to contract or take it out.

Put the checklist where people write, as a pinned note, a card, or an automated pre-send prompt, so it becomes a habit rather than a memory test.

Track the patterns you see. Where the same wording recurs, that is a training and process signal, not an individual failing.

Part 5

Making it a habit

Training is periodic; risk is continuous. A rule learned in spring does not stop a sentence typed in autumn, when someone is busy and trying to help. The only place to catch the wording is the moment it is written, which is why the checklist and the wording standard matter more than another annual module.

The habit matters more than any tool. Whether your team runs the checklist by hand or automates the check at the point of writing, for example a pre-send check inside Outlook that flags the phrase and offers a compliant version, the principle is the same: read the draft as a stranger would, treat absolute words as a stop sign, and catch the line before it leaves the building.

VerbaPulse

About VerbaPulse

The control this guide describes, built into the moment of writing.

Everything in this guide can be practised by hand: read the draft as a stranger would, run the checklist, hold the wording standard. VerbaPulse is what that discipline looks like when it runs automatically, at the point where the wording is chosen. It is a pre-send compliance check that works inside Outlook and Gmail while a person writes. It reads the draft against a library of legal and compliance risk patterns and against your own policies, highlights the exact phrase, explains in plain language why it is a problem, and offers a compliant rewrite or a clean removal. The writer keeps the final decision. It never sends, blocks, or rewrites on its own.

How it maps to this guide

The six patterns (Part 2)

Competition and antitrust, market abuse and inside information, financial promotions and performance claims, AML and tipping-off, client confidentiality and data, and binding commitments are the categories VerbaPulse is built to catch. Where a compliant rewrite exists, it offers one; where the whole sentence is the problem, it says so and recommends removal, using the same reasoning as the fix principles above.

The enforcement cases (Part 3)

The thread running through them is a control that did not exist at the moment of action. VerbaPulse puts a control at the moment of writing, the one place where email risk is actually created. It will not fix a channel-governance failure or an onboarding process, and it does not claim to. Its scope is the draft in front of the writer.

The toolkit (Part 4)

The checklist and the wording standard are the manual version of the check VerbaPulse runs. Your own policies, NDA lists, and house rules can be loaded so the check reflects your standard rather than a generic one, and every flag becomes anonymised evidence: a view of where language risk recurs, by team and category, with no email content stored.

The habit (Part 5)

Training is periodic; the check is continuous. Putting it where people write turns the habit from a memory test into a default.

Built to pass a compliance and security review

- Processing runs on Microsoft Azure OpenAI hosted in the EU (Sweden). Drafts are not sent to any US consumer AI service.
- Email content is analysed in memory and discarded. Only anonymised metadata about the risk, category, count, and team is retained, never the text of the message.
- It does not sit in the mail flow: it does not delay, quarantine, or read mailboxes in the background. It looks only at the draft in front of the writer, while they write.
- A Data Processing Agreement is available, and the processing model is designed to map to ISO 27002 controls and GDPR expectations.
- Stated plainly: VerbaPulse is certified and listed on Microsoft AppSource and is a verified Microsoft publisher. Microsoft 365 Certification, SOC 2, and ISO 27001 are on the roadmap and not yet held.

See it on your own drafts

Paste any email into the live demo at **verbapulse.com/go/try** and watch what it flags and how it rewrites it. For a guided walkthrough with your own policies, the DPA and ISO 27002 control mapping go out before any call.

Run it on real work:
Proof-of-Value Pilot

€120 flat for 30 days, up to 10 users, full platform access

- **Concierge onboarding:** we help configure your guidelines and set up your team. Most teams are live in a day, with no change to how mail is sent.
- A risk summary on day 25, so you see what it caught and where language risk concentrated.
- No auto-renewal and no minimum commitment. If you move to a Business plan afterwards, the €120 is credited to your first invoice.

VerbaPulse

verbapulse.com
hello@verbapulse.com
+372 636 0847

Business Inquiries
alican.elagoz@verbapulse.com
bill.m@verbapulse.com

VerbaPulse OÜ
Private limited company (osaühing) registered in the Republic of Estonia

Sepapaja tn 6, Lasnamäe linnaosa, 15551 Tallinn, Estonia
Registry code: 17552382
Registered at: Tartu Maakohtu registriosakond