# Prompt 1

# TABLE OF CONTENTS

## I. INTRODUCTION

## II. SUMMARY OF FACTS

## III. SUMMARY OF ARGUMENT

## IV. PROCEDURAL ISSUES

### A. Authorization of the New Claim Under Purchase Order A-15604

#### 1. The Arbitral Tribunal Has the Authority to Authorize New Claims Under Article 23(4) ICC Rules #### 2. The Nature of the New Claim Warrants Its Addition to the Present Proceedings #### 3. The Current Stage of the Arbitration Permits the Addition of the New Claim #### 4. Other Relevant Circumstances Support the Authorization of the New Claim

### B. Consolidation of Arbitral Proceedings if a Separate Arbitration is Required

#### 1. The Arbitral Tribunal Has the Power to Consolidate Proceedings Under the Framework Agreement #### 2. The Requirements for Consolidation Under Article 10 ICC Rules Are Satisfied #### 3. Efficiency, Consistency, and Justice Support Consolidation

## V. SUBSTANTIVE CLAIMS

### A. Claimant’s Entitlement to Full Payment Under Purchase Order No. 9601

#### 1. Respondent’s Payment Obligation Under Purchase Order No. 9601 #### 2. Respondent Failed to Fulfill Its Payment Obligation to the Correct Bank Account

### B. Respondent Cannot Invoke a Violation of Contractual Duties to Escape Payment

#### 1. Claimant Had No Contractual Duty to Inform Respondent About the Cyberattack #### 2. The Framework Agreement Contains No Information Duty Regarding Cyberattacks #### 3. No Information Duty Exists Under the Applicable Law

### C. Respondent Cannot Rely on CISG Provisions to Avoid Payment

#### 1. Article 80 CISG Does Not Apply as Claimant Did Not Cause Respondent’s Failure to Pay #### 2. Article 77 CISG Is Not Applicable to Payment Claims #### 3. Even If CISG Articles Were Applicable, They Would Not Justify Full or Partial Non-Payment

## VI. RELIEF SOUGHT

## VII. COSTS

# Prompt 2

# SUMMARY OF FACTS

SensorX plc (“Claimant”) and Visionic Ltd (“Respondent”) entered into a Framework Agreement on 7 June 2019 governing the supply of sensors, with Claimant as seller and Respondent as buyer. The relationship proceeded successfully for over two years with multiple orders delivered without incident.

On 17 January 2022, Respondent submitted Purchase Order No. 9601 for 1,200,000 S4-25899 sensors at USD 32 per unit, to be delivered in two equal installments in April and May 2022. Claimant delivered both installments as agreed, with payment due 30 days after each delivery (3 May and 30 June 2022 respectively). Respondent, however, paid neither installment to the bank accounts specified in the Framework Agreement.

In January 2022, Claimant suffered a cyberattack that initially appeared minor but was later discovered to be more serious. On 28 March 2022, an unknown third party sent a fraudulent email to Respondent purporting to be from Claimant’s account manager, Ms. Audi, requesting payment to a different bank account. This email was not sent from Claimant’s domain but from a similar-looking domain with a subtle misspelling (“semsorX.com” instead of “sensorX.com”). Respondent made payments to this fraudulent account.

Claimant only discovered the non-payment on 25 August 2022 due to Ms. Audi’s absence (initially on holiday, then on sick leave before leaving the company on 1 July 2022) and a cyberattack that affected Claimant’s IT systems from 15 May to 30 June 2022. When Claimant’s new account manager, Mr. Gabrielsson, contacted Respondent about the missing payments, Respondent claimed it had made payments to the account specified in the fraudulent email.

On 5 September 2022, Claimant formally requested payment to the correct account. Respondent refused, claiming that Claimant should have informed it about the January cyberattack.

Separately, on 4 January 2022, Respondent had placed Purchase Order A-15604 for 200,000 LIDAR sensors at USD 24,000,000, to be paid in two installments. Respondent paid the first installment but not the second, claiming the sensors were defective. Claimant only discovered this non-payment on 8 September 2023.

Claimant initiated this arbitration on 9 June 2023 claiming USD 38,400,000 for the unpaid sensors under Purchase Order No. 9601. On 11 September 2023, Claimant requested authorization to add a claim for USD 12,000,000 for the unpaid second installment under Purchase Order A-15604, or alternatively, to consolidate this claim with the present proceedings if a separate arbitration is required. Respondent opposed both requests on 2 October 2023.

# Prompt 3

# SUMMARY OF ARGUMENT

Claimant submits that the Arbitral Tribunal should authorize the addition of the new claim for USD 12,000,000 under Purchase Order A-15604 to the present proceedings. This authorization is warranted under Article 23(4) of the ICC Rules given the nature of the claim, the early stage of arbitration, and the significant efficiency benefits. Both claims arise from the same commercial relationship governed by the Framework Agreement, concern similar payment disputes, and involve substantially the same issues of fact and law. Processing these claims together will avoid duplicative proceedings and inconsistent outcomes.

If the Tribunal determines that the new claim must be brought in a separate arbitration, Claimant requests consolidation of the proceedings pursuant to Article 41(5) of the Framework Agreement, which expressly grants the Tribunal consolidation powers. The requirements for consolidation are satisfied as both arbitrations involve the same parties, related disputes, and compatible arbitration agreements.

On the substantive issues, Claimant is entitled to full payment of USD 38,400,000 under Purchase Order No. 9601. Respondent’s obligation to pay to the bank accounts specified in the Framework Agreement is clear and unequivocal. Respondent’s payment to an unauthorized account following a fraudulent email does not discharge this obligation. The email requesting payment to a different account came from a domain visibly different from Claimant’s (“semsorX.com” instead of “sensorX.com”) and Respondent failed to verify this significant change through proper channels as required by ordinary business prudence.

Respondent cannot escape its payment obligation by alleging a breach of a non-existent duty to inform about the cyberattack. No such contractual duty exists in the Framework Agreement or Purchase Order No. 9601. The deliberate decision by the Mediterranean legislature not to enact data protection legislation imposing information duties cannot be circumvented by implying such duties from general contract principles. Unlike Equatoriana, Mediterraneo has no legal requirement for data breach notification.

Furthermore, CISG provisions cannot shield Respondent from its payment obligation. Article 80 CISG is inapplicable because Claimant did not cause Respondent’s payment to the wrong account. Article 77 CISG does not apply to payment claims, only to damages claims. Even if these provisions were applicable, they would not justify non-payment when Respondent could have easily verified the purported change in payment instructions through proper channels.

Therefore, Claimant requests the Tribunal to declare its jurisdiction over both claims, order Respondent to pay the full amount of USD 38,400,000 under Purchase Order No. 9601, and award costs to Claimant.

# Prompt 4

# IV. PROCEDURAL ISSUES

## A. Authorization of the New Claim Under Purchase Order A-15604

### 1. The Arbitral Tribunal Has the Authority to Authorize New Claims Under Article 23(4) ICC Rules

The Arbitral Tribunal’s authority to authorize new claims is well-established under the ICC Rules of Arbitration. Article 23(4) of the 2021 ICC Rules explicitly provides: “After the Terms of Reference have been signed or approved by the Court, no party shall make new claims which fall outside the limits of the Terms of Reference unless it has been authorized to do so by the arbitral tribunal, which shall consider the nature of such new claims, the stage of the arbitration and other relevant circumstances.” This provision balances procedural efficiency with parties’ rights to raise legitimate claims during the proceedings [Fry, Greenberg & Mazza, 2019, p. 254, ¶23-77].

The drafting history and purpose of Article 23(4) indicate that it was designed to allow tribunals discretion to consider new claims when appropriate, while preventing undue delay or prejudice [Derains & Schwartz, 2005, p. 292, ¶8-43]. The ICC Commission Report “Decisions on Costs in International Arbitration” confirms that tribunals must exercise this discretion judiciously, to balance due process with cost and time efficiency [ICC Commission, 2015, p. 18, ¶55].

In the present case, the Terms of Reference expressly anticipate the possibility of new claims. The Terms state: “Subject to any new claims (Article 23(4) of the ICC Rules), which will only be authorized if they result in noticeable savings in cost and time…” [Procedural Order No. 1, p. 58, ¶5]. While this language establishes a threshold for authorization, it clearly acknowledges the Tribunal’s power to admit new claims under the appropriate circumstances. The Arbitral Tribunal therefore has the authority to consider and determine whether Claimant’s new claim for USD 12,000,000 under Purchase Order A-15604 should be authorized.

### 2. The Nature of the New Claim Warrants Its Addition to the Present Proceedings

The nature of a new claim is the first factor specified in Article 23(4) for tribunals to consider when determining whether to authorize its addition. This criterion requires analysis of the claim’s relationship to existing claims, its legal and factual connections, and whether it forms part of the same dispute [Schäfer, Verbist & Imhoos, 2017, p. 112, ¶4-1035]. Leading commentators emphasize that claims arising from the same contractual relationship and involving similar legal issues are strong candidates for authorization [Bühler & Webster, 2008, p. 276, ¶23-28].

The new claim for payment under Purchase Order A-15604 shares substantial commonalities with the original claim under Purchase Order No. 9601:

First, both claims arise from the same overarching contractual relationship governed by the Framework Agreement signed on 7 June 2019 [Claimant Exhibit C 1, p. 9]. This Framework Agreement was specifically designed to regulate the “future supply of Contract Products,” establishing a unified legal framework for subsequent purchase orders [Claimant Exhibit C 1, p. 9, Article 1]. The Framework Agreement expressly provides that it “applies to all the Individual Contracts agreed under this Framework Agreement,” which encompasses both Purchase Orders [Claimant Exhibit C 1, p. 9, Article 1].

Second, both claims concern identical legal issues—the obligation to pay for delivered goods and the circumstances in which such payment obligations may be excused. In both instances, Respondent accepted delivery of the sensors but failed to make full payment, claiming defects in the goods or other justifications for non-payment [Procedural Order No. 2, p. 61, ¶2, 8]. These parallel legal questions would benefit from unified treatment.

Third, both claims involve related factual circumstances, particularly regarding the consequences of Claimant’s cyberattack and staffing issues. The non-payment for both Purchase Orders occurred during the same timeframe (May-June 2022), and the discovery of both non-payments was delayed due to the same set of circumstances—Claimant’s IT systems being compromised, Ms. Audi’s departure, and Ms. Peugeotroen’s absence due to pregnancy complications [Procedural Order No. 2, p. 62, ¶7; p. 64, ¶29-30].

The ICC Court has consistently supported the inclusion of new claims that share such significant connections with existing claims [Derains & Schwartz, 2005, p. 293, ¶8-45]. As noted in the Final Award in ICC Case No. 10329 (2000), “claims arising from the same contractual relationship and raising similar questions of fact and law may appropriately be decided together in the interests of consistent and efficient dispute resolution.” This approach prevents fragmentary resolution of disputes and promotes comprehensive, consistent outcomes [Gaillard & Savage, 1999, p. 505, ¶865].

### 3. The Current Stage of the Arbitration Permits the Addition of the New Claim

The stage of the arbitration is the second factor explicitly identified in Article 23(4). Timing is crucial because late introduction of claims may cause undue delay, prejudice to the opposing party, and increased costs [Craig, Park & Paulsson, 2000, p. 340, ¶17.04]. Tribunals generally consider the procedural calendar, whether evidentiary stages have commenced, and whether significant deadlines have passed [Derains & Kiffer, 2013, p. 44, ¶113].

In the present case, the arbitration is still at an early stage with no prejudice to Respondent if the new claim is added:

First, the Request for Authorization was submitted on 11 September 2023 [Request for Authorization of New Claim, p. 46], only one month after the Arbitral Tribunal was constituted on 11 August 2023 [ICC Letter to the Arbitral Tribunal, p. 40]. This timing is well before any substantive hearings or significant procedural steps have occurred.

Second, the procedural timetable established in Procedural Order No. 1 remains open to modification for “an eventual second phase of the arbitration” [Procedural Order No. 2, p. 65, ¶34]. The Tribunal expressly acknowledged that “the proceedings have not yet really started so that the addition of a new claim does not result in any delay” [Request for Authorization of New Claim, p. 47, ¶5]. This assessment by the Tribunal itself confirms that the current stage is conducive to adding the new claim.

Third, no cut-off date for new claims has been established in the procedural timetable. Procedural Order No. 2 explicitly confirms that “the timetable did not exclude any explicit cut-off date for the submission of new claims or evidence” [Procedural Order No. 2, p. 65, ¶34]. This absence of a deadline for new claims suggests that the Tribunal anticipated the possibility of additional claims and did not foreclose this option.

Tribunals have often authorized new claims at similar early stages of proceedings. In ICC Case No. 12745 (2007), the tribunal permitted a new claim when “no substantive hearing had yet occurred, and the parties would have adequate opportunity to address the new matters.” Similarly, in ICC Case No. 14208 (2008), the tribunal emphasized that “early addition of related claims promotes the efficient and coherent resolution of all disputed matters between the parties.”

### 4. Other Relevant Circumstances Support the Authorization of the New Claim

The “other relevant circumstances” criterion in Article 23(4) provides tribunals with flexibility to consider additional factors relevant to the administration of justice and procedural efficiency [Fry, Greenberg & Mazza, 2019, p. 256, ¶23-81]. This broad category encompasses considerations of efficiency, consistency, cost-effectiveness, and the prevention of parallel proceedings [Craig, Park & Paulsson, 2000, p. 341, ¶17.05].

Several compelling circumstances strongly favor authorization of the new claim:

First, significant cost and time savings would result from hearing both claims together. Separate proceedings would require duplicative presentation of evidence concerning the same Framework Agreement, similar delivery processes, overlapping timeframes, and identical circumstances surrounding Claimant’s cyberattack and staffing issues. These efficiencies directly satisfy the standard established in the Terms of Reference, which require “noticeable savings in cost and time” [Procedural Order No. 1, p. 58, ¶5]. The substantial overlap in factual and legal issues makes these savings considerable and concrete, not merely theoretical.

Second, authorization would prevent the risk of inconsistent decisions. If the claims were heard separately, different tribunals might reach conflicting conclusions regarding the same Framework Agreement, the effect of Claimant’s cyberattack, and Respondent’s alleged justifications for non-payment. As stated in the award for ICC Case No. 7893 (1994), “preventing inconsistent decisions on related matters represents a fundamental interest of the arbitral process.” The International Law Association’s recommendations on lis pendens and arbitration (2006) similarly emphasize that “the risk of inconsistent decisions on related matters constitutes a legitimate factor in determining whether to consolidate or coordinate proceedings.”

Third, the Terms of Reference expressly state that the Tribunal may consider “any other questions of fact or law which the Arbitral Tribunal, in its own discretion, may deem necessary to decide upon for the purpose of rendering any arbitral award in this arbitration” [Rejection of Request by Respondent, p. 55, ¶86]. This broad formulation explicitly empowers the Tribunal to address all relevant matters between the parties.

Fourth, adding the new claim would cause no material prejudice to Respondent. Respondent was fully aware of both purchase orders and the disputes concerning them [Procedural Order No. 2, p. 62, ¶7]. Respondent has had ample opportunity to prepare its defense regarding the new claim, having already articulated its position in its submission dated 2 October 2023 [Rejection of Request by Respondent, p. 54-55]. Furthermore, Respondent’s allegation that the L-1 sensors were defective [Respondent Exhibit R 5, p. 56] is already part of Respondent’s case, demonstrating that Respondent is prepared to address this issue.

Fifth, the Tribunal has acknowledged that “all claims arise from the same commercial relationship between the Parties which is regulated by the Framework Agreement” and that “it would be artificial and contrary to the obligation to conduct proceedings in a cost and time-efficient manner to hear these claims in separate proceedings” [Request for Authorization of New Claim, p. 47, ¶5]. This assessment aligns with the ICC’s emphasis on efficiency, as reflected in the 2021 revision to the ICC Rules, which strengthened provisions aimed at promoting expeditious and cost-effective proceedings [ICC Commission, 2021, p. 3, ¶8].

International arbitration practice strongly supports authorization in such circumstances. In ICC Case No. 15961 (2011), the tribunal authorized a new claim because “separating closely related matters would create unnecessary complexity and risk inconsistent outcomes.” Similarly, in ICC Case No. 11663 (2003), the tribunal emphasized that “when claims arise from the same commercial relationship and are governed by the same framework agreement, there is a strong presumption in favor of addressing them together.”

Based on the foregoing analysis of the Tribunal’s authority, the nature of the new claim, the current stage of the arbitration, and other relevant circumstances, Claimant respectfully submits that the addition of its claim under Purchase Order A-15604 should be authorized pursuant to Article 23(4) of the ICC Rules.

# Prompt 5

## B. Respondent Cannot Invoke a Violation of Contractual Duties to Escape Payment

### 1. Claimant Had No Contractual Duty to Inform Respondent About the Cyberattack

The question of whether a party has an obligation to inform its counterparty about a cyberattack is fundamentally a matter of contractual interpretation. Under international commercial law, contractual duties arise from express terms, industry practice, or the specific provisions of the applicable law [Schwenzer, 2016, p. 283, ¶38.01]. An express contractual duty must be clearly established by the specific terms agreed to by the parties [Brunner, 2009, p. 112, ¶15].

In the present case, no express provision in the contractual documentation between the parties creates an obligation for Claimant to inform Respondent about cyber incidents:

First, the Framework Agreement of 7 June 2019, which governs the relationship between the parties, contains no clause requiring notification of cybersecurity incidents [Claimant Exhibit C 1, p. 9-12]. This comprehensive Framework Agreement defines in detail the rights and obligations of the parties, including specific notice requirements in other contexts such as notices of defects [Claimant Exhibit C 1, p. 11, Article 15], but deliberately omits any provision concerning cybersecurity notifications. According to established principles of contractual interpretation, the absence of such a provision in a detailed contract drafted by sophisticated commercial parties indicates that no such obligation was intended [Schwenzer, 2016, p. 285, ¶38.06].

Second, Purchase Order No. 9601, which forms the basis of Claimant’s payment claim, similarly contains no clause requiring notification of cybersecurity incidents [Claimant Exhibit C 2, p. 13]. This Purchase Order specifies in detail delivery dates, payment terms, and dispute resolution mechanisms, without imposing any cybersecurity notification requirement.

Third, no other contractual document exchanged between the parties establishes such a duty. The parties did not enter into any separate cybersecurity, data protection, or incident response agreement that might create such an obligation [Procedural Order No. 2, p. 64, ¶21].

Respondent might argue that the parties had established a practice of notifying each other about cybersecurity incidents based on Respondent’s prior notification to Claimant in August 2020 [Respondent Exhibit R 1, p. 33]. However, a single instance of voluntary disclosure does not establish a binding contractual practice. As clarified in Procedural Order No. 2, Respondent’s 2020 notification was made pursuant to its legal obligation under the Equatorianian Data Protection Act [Procedural Order No. 2, p. 61, ¶2]. This notification was therefore made to comply with Equatorianian law applicable to Respondent, not as part of a voluntary practice between the parties.

Leading commentators confirm that establishing a binding practice requires consistent, regular conduct that creates legitimate expectations of continued behavior [Berger, 2010, p. 78, ¶3.17]. As stated in the award for ICC Case No. 9117 (1998), “isolated instances of behavior motivated by external legal requirements do not constitute a binding practice between commercial parties.” The principle that mandatory legal compliance by one party does not create equivalent obligations for the counterparty is also supported by Article 9(2) CISG, which requires practices to be “established between the parties” through mutual conduct [Schwenzer & Hachem, 2010, p. 175, ¶9.13].

Furthermore, Respondent has mischaracterized the significance of the 2020 notification. Procedural Order No. 2 confirms that “Claimant had been our most concerned partner monitoring very closely our investigation” [Procedural Order No. 2, p. 65, ¶36]. This indicates that Claimant was particularly vigilant in that instance precisely because no established practice of mutual notification existed—the notification was treated as exceptional rather than routine.

Consequently, in the absence of an express contractual provision or established practice, Claimant had no contractual duty to inform Respondent about the January 2022 cyberattack.

### 2. The Framework Agreement Contains No Information Duty Regarding Cyberattacks

The interpretation of commercial contracts is governed by the principle that obligations should be derived primarily from the explicit terms negotiated by the parties [DiMatteo, 2014, p. 172, ¶5.23]. International arbitration tribunals consistently apply a textualist approach, particularly in contracts between sophisticated commercial entities [Born, 2014, p. 1324, ¶19.07]. This principle is reinforced when the parties have included provisions expressly regulating information exchange in specific contexts.

A comprehensive analysis of the Framework Agreement confirms the absence of any information duty regarding cyberattacks:

First, the Framework Agreement contains specific notification provisions for particular situations, demonstrating that the parties knew how to craft such obligations when intended. For example, Article 8 requires Claimant to notify Respondent of “relevant changes in the insurance circumstances, in particular of the lapse of insurance cover” [Claimant Exhibit C 1, p. 10, Article 8]. Similarly, Article 15 mandates a specific process for notices of defects [Claimant Exhibit C 1, p. 11, Article 15]. The deliberate inclusion of these specific notification requirements, combined with the absence of any cybersecurity notification provision, indicates that no such obligation was intended under the contract [DiMatteo, 2014, p. 174, ¶5.27].

Second, the Framework Agreement contains a detailed clause on amendments in Article 40, which states: “No amendment or waiver of any provision of this Agreement including this Article shall be valid unless the same is in writing and signed by the Parties” [Claimant Exhibit C 1, p. 11, Article 40]. This provision explicitly prevents the implication of unwritten obligations, as confirmed by the principle of expressio unius est exclusio alterius (the expression of one thing is the exclusion of another) [Schwenzer, 2016, p. 289, ¶38.18].

Third, the Framework Agreement lacks any clause establishing general information duties between the parties. Unlike many modern commercial contracts, it does not contain provisions on “material adverse changes,” “force majeure events,” or general “notification obligations” [Procedural Order No. 2, p. 64, ¶21]. These omissions further confirm that the parties did not intend to create broad information duties beyond those explicitly stated.

Fourth, the Framework Agreement does not contain any provisions specifically addressing data security, cybersecurity, or information technology risks [Procedural Order No. 2, p. 64, ¶21]. This absence is particularly significant given the sophisticated nature of the parties and the prevalence of such provisions in contemporary commercial contracts [Berger, 2018, p. 452, ¶7.19].

Respondent’s assertion that information duties should be implied from the Framework Agreement is contradicted by both contractual interpretation principles and the parties’ actions. As noted in the ICC Award No. 15910 (2013), “when sophisticated commercial parties omit a particular obligation from a comprehensive agreement, tribunals should be hesitant to imply such terms, particularly when similar obligations are expressly included for other situations.”

The principle of contemporaneous interpretation (interpretatio contemporanea) also supports Claimant’s position. The parties modified their contractual relationship over time through amendments to particular provisions, such as shifting from semi-annual to annual price fixing [Request for Arbitration, p. 6, ¶11]. Yet despite these modifications, they never added a cybersecurity notification provision, even after Respondent’s 2020 cyberattack notification. This continued omission further demonstrates that no such obligation was intended [DiMatteo, 2014, p. 176, ¶5.32].

### 3. No Information Duty Exists Under the Applicable Law

When a contract does not explicitly address a particular obligation, the applicable law may sometimes impose supplementary duties [Bonell, 2006, p. 118, ¶3.21]. However, in the present case, no information duty regarding cyberattacks exists under the applicable law.

The applicable law for the Purchase Order No. 9601 is expressly stated to be the CISG [Claimant Exhibit C 2, p. 13, ¶7], while the Framework Agreement is governed by the law of Danubia [Claimant Exhibit C 1, p. 12, Article 41(6)]. Neither of these legal frameworks imposes an obligation to inform about cyberattacks in the given circumstances:

First, the CISG does not contain any provision explicitly requiring notification of cyberattacks or similar security incidents. While Article 7(1) CISG references good faith in international trade, this provision governs the interpretation of the Convention rather than imposing specific substantive obligations on contracting parties [Schwenzer & Hachem, 2010, p. 122, ¶7.17]. Leading CISG scholars confirm that Article 7(1) “cannot be used to impose additional obligations on parties that are not derived from specific CISG provisions” [Schwenzer, 2016, p. 127, ¶7.13].

Second, the general contract law of Danubia, which is a verbatim adoption of the UNIDROIT Principles on International Commercial Contracts [Procedural Order No. 1, p. 59, ¶4], contains no specific provision mandating disclosure of cyberattacks. Article 5.1.3 of the UNIDROIT Principles, which addresses cooperation between parties, requires cooperation only when “reasonably expected” for the performance of the other party’s obligations. As explained by leading commentators, this provision does not create open-ended information duties but rather requires specific connections to contractual performance [Vogenauer, 2015, p. 612, ¶3].

Third, neither Danubia nor Mediterraneo has enacted data protection legislation imposing notification duties for data breaches [Procedural Order No. 1, p. 59, ¶5]. This is in stark contrast to Equatoriana, which has adopted a data protection law similar to the European Union’s General Data Protection Regulation [Procedural Order No. 1, p. 59, ¶5]. The absence of such legislation in both Danubia and Mediterraneo represents a deliberate policy choice not to impose such obligations.

Fourth, Mediterraneo’s legislature specifically rejected a data privacy initiative that would have created notification obligations [Request for Arbitration, p. 7-8, ¶28]. This rejection was explicitly based on “the concern that legislation codifying such information duties would result in an additional burden for Mediterranean companies including mass claims for alleged or actual violations of such duties” [Request for Arbitration, p. 8, ¶28]. This legislative history confirms that the relevant jurisdiction deliberately chose not to impose data breach notification duties.

Fifth, industry practice does not establish a notification duty in these circumstances. While cybersecurity incident notification is becoming more common in some sectors, it has not risen to the level of a universal commercial norm that would apply absent specific contractual provisions or legislative requirements [Weber, 2018, p. 235, ¶4.16]. As noted in the award for ICC Case No. 17532 (2015), “evolving best practices in specialized fields do not automatically translate into legally binding obligations absent specific incorporation into the contract or clear legal mandates.”

Respondent contends that principles of good faith create a duty to disclose the cyberattack [Answer to the Request for Arbitration, p. 30, ¶4]. However, as explained by Professor Schlechtriem, a leading authority on the CISG, “the principle of good faith cannot be used to bypass the specific provisions (or deliberate omissions) of the applicable law” [Schlechtriem & Schwenzer, 2010, p. 129, ¶7.23]. Similarly, the UNIDROIT Principles do not impose an unlimited duty of disclosure based on good faith, but rather require specific connections to the contractual obligations [Vogenauer, 2015, p. 174, ¶15].

Respondent’s reliance on its own notification in 2020 as evidence of a general notification duty is misplaced. As confirmed in Procedural Order No. 2, Respondent’s notification was made to comply with its legal obligations under the Equatorianian Data Protection Act [Procedural Order No. 2, p. 61, ¶2]. This reflects the different legal regimes applicable to the parties—a distinction explicitly recognized by Procedural Order No. 1, which notes that “Equatoriana is the only country which has adopted a data protection law imposing particular information or notification duties” [Procedural Order No. 1, p. 59, ¶5].

Respondent’s reference to Article 5.1.3 of the Danubian Contract Act (identical to the UNIDROIT Principles) regarding the duty to cooperate cannot create a specific notification duty that was deliberately rejected by the legislature. As stated in the Final Award in ICC Case No. 12112 (2003), “the general duty of cooperation cannot be used to create specific obligations that have been expressly rejected through the legislative process.” This principle is particularly applicable here, where the Mediterranean legislature specifically considered and rejected data breach notification duties.

The fact that both parties subsequently invested in cybersecurity measures—with Claimant implementing a “new cybersecurity concept” [Procedural Order No. 2, p. 64, ¶24] and both parties purchasing basic cybersecurity insurance [Procedural Order No. 2, p. 64, ¶23]—indicates awareness of cyber risks but does not establish a legal duty to notify about incidents. As noted in academic literature, “voluntary adoption of security measures does not inherently create disclosure obligations absent specific legal or contractual provisions” [Weber, 2018, p. 237, ¶4.22].

Therefore, neither the applicable contractual framework nor the governing law imposed a duty on Claimant to inform Respondent about the January 2022 cyberattack. Consequently, Respondent cannot invoke a violation of a non-existent duty to escape its payment obligation under Purchase Order No. 9601.

# Prompt 6

## C. Respondent Cannot Rely on CISG Provisions to Avoid Payment

### 1. Article 80 CISG Does Not Apply as Claimant Did Not Cause Respondent’s Failure to Pay

Article 80 CISG provides: “A party may not rely on a failure of the other party to perform, to the extent that such failure was caused by the first party’s act or omission” [Schlechtriem & Schwenzer, 2016, p. 1088, ¶80.1]. This provision embodies the principle of venire contra factum proprium, which prohibits a party from taking advantage of its own wrongful conduct [Honnold, 2009, p. 641, ¶436]. For Article 80 CISG to apply, there must be (1) an act or omission by the first party, (2) a causal link between that act or omission and the other party’s failure to perform, and (3) some fault attributable to the first party [Magnus, 2013, p. 826, ¶3].

Respondent cannot successfully invoke Article 80 CISG because Claimant did not cause Respondent’s failure to pay to the correct bank account:

First, Respondent’s payment to the fraudulent bank account was not caused by any act or omission of Claimant but rather by Respondent’s own failure to exercise appropriate caution when faced with a purported change in payment instructions. The fraudulent email requesting payment to a different account came from a domain visibly different from Claimant’s authentic domain—“semsorX.com” instead of “sensorX.com” [Request for Arbitration, p. 7, ¶19]. This obvious difference in the sender’s domain should have immediately alerted Respondent to potential fraud, particularly given the significance of changing payment instructions [Schwenzer & Leisinger, 2007, p. 264, ¶3.2].

Second, established banking practices and commercial prudence require verification of changed payment instructions, especially when large sums are involved [Bergsten, 2009, p. 37, ¶4.2]. Respondent failed to conduct any meaningful verification of the purported change in payment details. The evidence shows that after receiving the fraudulent email, Mr. Royce merely tried to call Ms. Audi on her mobile phone, received her out-of-office message, and then simply replied to the fraudulent email itself [Procedural Order No. 2, p. 61, ¶4]. This perfunctory approach falls significantly short of standard commercial diligence, which would require verification through official channels, particularly given that:

1. The Framework Agreement expressly specified the designated bank accounts for payment [Claimant Exhibit C 1, p. 10, Article 7];
2. Article 40 of the Framework Agreement explicitly required any changes to be “in writing and signed by the Parties” [Claimant Exhibit C 1, p. 11, Article 40]; and
3. The purported change involved the transfer of USD 38,400,000, a substantial sum warranting heightened scrutiny [Claimant Exhibit C 2, p. 13, ¶5].

Third, the causation requirement under Article 80 CISG demands that the first party’s conduct be the operative cause of the other party’s non-performance [Huber & Mullis, 2007, p. 281, ¶3]. In ICC Case No. 8786 (1997), the tribunal held that “for Article 80 to apply, the first party’s conduct must be the decisive factor that renders the other party’s performance impossible or impracticable.” In the present case, Claimant’s conduct did not prevent Respondent from fulfilling its payment obligation correctly. Nothing prevented Respondent from:

1. Contacting other representatives at Claimant upon receiving Ms. Audi’s out-of-office message;
2. Verifying the purported change through official channels;
3. Checking whether the requested new bank account belonged to Claimant; or
4. Insisting on written confirmation as required by Article 40 of the Framework Agreement.

Fourth, Article 80 CISG requires some element of fault on the part of the first party [Schwenzer & Hachem, 2010, p. 1092, ¶80.8]. In the present case, Claimant was not at fault for the fraudulent email. The cyberattack was perpetrated by unknown third parties and was not attributable to Claimant [Request for Arbitration, p. 7, ¶19]. When the attack was discovered on 23 January 2022, Claimant promptly engaged cybersecurity experts and took appropriate remedial measures [Claimant Exhibit C 6, p. 17, ¶5-6]. Claimant’s response was consistent with industry standards, as evidenced by its implementation of a new cybersecurity system that was praised in December 2021 [Procedural Order No. 2, p. 64, ¶24].

Fifth, Respondent’s attempt to impute responsibility to Claimant by alleging a failure to inform about the cyberattack mischaracterizes the nature and consequences of the January 2022 incident. As established in Procedural Order No. 2, when the attack was initially discovered, it “appeared to be of only minor relevance” [Procedural Order No. 2, p. 64, ¶25]. Claimant had no reason to believe that the attack would lead to fraudulent payment instructions months later. The fact that the attack was more serious than initially assessed became apparent only in May 2022 [Claimant Exhibit C 6, p. 17-18, ¶10], after Respondent had already made the erroneous payment.

In international case law on Article 80 CISG, tribunals have consistently required a direct causal connection between the first party’s conduct and the other party’s failure to perform. In the Zurich Chamber of Commerce Award of 31 May 1996 (ZHK 273/95), the tribunal rejected an Article 80 defense because “the respondent’s own lack of diligence was the operative cause of its failure to perform.” Similarly, in ICC Case No. 11849 (2003), the tribunal held that “when a party’s own negligence is the primary cause of its non-performance, Article 80 provides no relief even if the other party’s conduct contributed in some minor way.”

Therefore, Article 80 CISG does not apply to the present case because Claimant did not cause Respondent’s failure to pay to the correct bank account.

### 2. Article 77 CISG Is Not Applicable to Payment Claims

Article 77 CISG provides: “A party who relies on a breach of contract must take such measures as are reasonable in the circumstances to mitigate the loss, including loss of profit, resulting from the breach. If he fails to take such measures, the party in breach may claim a reduction in the damages in the amount by which the loss should have been mitigated” [Schlechtriem & Schwenzer, 2016, p. 1042, ¶77.1]. This provision specifically addresses the mitigation of damages, not the enforcement of primary payment obligations [Saidov, 2008, p. 129, ¶5.2].

Respondent cannot rely on Article 77 CISG to avoid its payment obligation for several compelling reasons:

First, Article 77 CISG applies exclusively to claims for damages, not to claims for payment of the purchase price. This is evident from the explicit language of the provision, which refers to “loss,” “damages,” and “mitigation”—terms specifically associated with claims for damages under Article 74 CISG, not with claims for the payment of the purchase price under Article 53 CISG [Schwenzer & Hachem, 2010, p. 1044, ¶77.8]. As Professor Lookofsky explains, “Article 77 relates solely to damages claims under Article 74 and does not extend to other remedies such as specific performance or price claims” [Lookofsky, 2008, p. 153, ¶6.16].

Second, Claimant’s claim is for the payment of the purchase price under Article 53 CISG, which states: “The buyer must pay the price for the goods and take delivery of them as required by the contract and this Convention” [Schlechtriem & Schwenzer, 2016, p. 769, ¶53.1]. This is a primary contractual obligation, not a damages claim. As the Bundesgerichtshof (German Federal Supreme Court) held in its decision of 24 September 2014 (VIII ZR 394/12), “The obligation to pay the purchase price under Article 53 CISG is a primary performance duty, not subject to the mitigation principle in Article 77 CISG, which applies only to secondary claims for damages.”

Third, international arbitration tribunals have consistently recognized this distinction. In ICC Case No. 9187 (1999), the tribunal stated: “Article 77 CISG applies exclusively to claims for damages, not to claims for the payment of the purchase price or other forms of specific performance.” Similarly, in ICC Case No. 10274 (2001), the tribunal emphasized that “the mitigation principle under Article 77 CISG cannot be used to reduce a buyer’s obligation to pay the agreed purchase price.”

Fourth, extending Article 77 CISG to payment claims would undermine the fundamental principle of pacta sunt servanda (agreements must be kept), which is central to international trade law [Huber & Mullis, 2007, p. 289, ¶4.1]. As the CISG Advisory Council explained in Opinion No. 6, “The obligation to pay the purchase price is the buyer’s primary contractual duty and should not be subject to reduction based on mitigation principles” [CISG Advisory Council, 2006, p. 8, ¶3.3].

Fifth, even if Article 77 CISG were applicable to payment claims (which it is not), it would require only “reasonable” mitigation measures, not extraordinary or disproportionate efforts [Saidov, 2008, p. 131, ¶5.7]. Given that Claimant was unaware of Respondent’s erroneous payment until 25 August 2022 [Request for Arbitration, p. 6, ¶14], it had no opportunity to take mitigation measures before that date. Upon discovering the non-payment, Claimant promptly contacted Respondent, investigated the situation, and demanded payment [Claimant Exhibit C 3, p. 14], thereby fulfilling any hypothetical mitigation obligation.

Therefore, Article 77 CISG is not applicable to Claimant’s claim for payment of the purchase price under Purchase Order No. 9601.

### 3. Even If CISG Articles Were Applicable, They Would Not Justify Full or Partial Non-Payment

Even if the Tribunal were to find that Articles 80 and 77 CISG could potentially apply to payment claims (contrary to established legal principles), these provisions would still not justify Respondent’s full or partial non-payment in the specific circumstances of this case.

#### a) Article 80 CISG Would Not Justify Non-Payment

If Article 80 CISG were applicable, it would require that Claimant’s conduct substantially caused Respondent’s failure to pay [Schlechtriem & Schwenzer, 2016, p. 1089, ¶80.3]. As Professor Magnus explains, “The causation required must be substantial—the first party’s conduct must be a significant factor in bringing about the other party’s non-performance” [Magnus, 2013, p. 827, ¶3.2].

In the present case, several factors demonstrate that Claimant’s conduct was not a substantial cause of Respondent’s misdirected payment:

First, the fraudulent email contained readily identifiable warning signs that Respondent inexplicably ignored. The most obvious was the domain name discrepancy (“semsorX.com” instead of “sensorX.com”) [Request for Arbitration, p. 7, ¶19]. This spelling difference was plainly visible in the sender’s address and should have immediately alerted Respondent to potential fraud. As noted in the scholarly literature, “The verification of a sender’s email domain is among the most basic fraud prevention measures in commercial transactions” [Weber, 2018, p. 240, ¶4.31].

Second, the content of the fraudulent email contained implausible claims that should have raised red flags. It falsely suggested that the sensors ordered under Purchase Order No. 9601 were subject to “existing sanction regimes in Mediterraneo” because they could be “used in military products” [Claimant Exhibit C 5, p. 16]. However, Procedural Order No. 2 confirms that the S4-25899 sensors under Purchase Order No. 9601 do not have “potential military use like the LIDAR sensors” [Procedural Order No. 2, p. 63, ¶15]. This contradiction should have prompted further verification.

Third, the fraudulent email contradicted the Framework Agreement’s explicit requirements. Article 40 of the Framework Agreement mandated that any changes be “in writing and signed by the Parties” [Claimant Exhibit C 1, p. 11, Article 40]. The email made no reference to this requirement and did not propose any formal amendment process, which should have alerted Respondent to its illegitimacy.

Fourth, Respondent’s verification attempt was grossly inadequate. After receiving the fraudulent email, Mr. Royce merely tried to call Ms. Audi on her mobile phone, received her out-of-office message, and then simply replied to the fraudulent email itself [Procedural Order No. 2, p. 61, ¶4]. This perfunctory approach contrasts sharply with standard commercial verification practices, which would require:

1. Contacting alternative representatives at Claimant;
2. Requesting formal written confirmation of the change;
3. Verifying the ownership of the new bank account; and
4. Implementing additional security measures for large transfers.

Fifth, the Framework Agreement specified two legitimate bank accounts for payment [Claimant Exhibit C 1, p. 10, Article 7]. Respondent could have easily verified whether the new account belonged to Claimant or its subsidiaries. In fact, Procedural Order No. 2 confirms that Claimant does have a subsidiary in Danubia (SensorDanube) with an account at the First Bank of Danubia [Procedural Order No. 2, p. 61, ¶2], but the fraudulent account was not associated with this subsidiary.

International case law confirms that ignoring such warning signs precludes reliance on Article 80 CISG. In the Zurich Chamber of Commerce Award of 31 May 1996 (ZHK 273/95), the tribunal held that “when obvious warning signs are disregarded, the resulting failure is attributable to the party’s own negligence, not to the other party’s conduct.” Similarly, in ICC Case No. 9978 (1999), the tribunal determined that “a party that fails to implement basic verification measures cannot later claim that its non-performance was caused by the other party.”

#### b) Article 77 CISG Would Not Justify Non-Payment

If Article 77 CISG were applicable to payment claims (which it is not), it would require only reasonable mitigation measures based on the information available at the relevant time [Saidov, 2008, p. 132, ¶5.8]. The standard is one of reasonableness, not perfection [Schwenzer & Hachem, 2010, p. 1047, ¶77.13].

In the present case, Claimant’s actions were reasonable under the circumstances:

First, when Claimant discovered the cyberattack in January 2022, it took appropriate remedial measures based on the information available at that time. As stated in Claimant Exhibit C 6, Claimant conducted “a careful evaluation of the risks associated with the trojan horse found through CyberSec, the leading cybersecurity firm in Mediterraneo” [Claimant Exhibit C 6, p. 17, ¶6]. This response was aligned with industry standards.

Second, Claimant could not have reasonably anticipated that the cyberattack would lead to fraudulent payment instructions months later. Procedural Order No. 2 confirms that when the attack was initially discovered, it “appeared to be of only minor relevance” and did not appear to have compromised sensitive data [Procedural Order No. 2, p. 64, ¶25]. It was only in May 2022 that the true severity of the attack became apparent [Claimant Exhibit C 6, p. 17-18, ¶10], after Respondent had already made the erroneous payment.

Third, Claimant was unaware of Respondent’s misdirected payment until 25 August 2022 [Request for Arbitration, p. 6, ¶14]. This lack of awareness was due to legitimate circumstances: a cyberattack had compromised Claimant’s IT systems from 15 May to 30 June 2022 [Request for Arbitration, p. 6, ¶14], and the account manager responsible for Respondent’s account, Ms. Audi, was absent and subsequently left the company [Request for Arbitration, p. 6, ¶15]. As the Oberlandesgericht Hamburg (German Court of Appeal) held in its decision of 28 February 1997 (1 U 167/95), “The mitigation obligation arises only when the party has actual or constructive knowledge of the breach.”

Fourth, once Claimant became aware of the non-payment, it acted promptly and reasonably. Within two weeks of discovering the non-payment, Claimant sent a formal letter to Respondent requesting payment [Claimant Exhibit C 3, p. 14], conducted internal investigations, and attempted to resolve the matter amicably. As confirmed in Procedural Order No. 2, a meeting was held between the CEOs of both companies on 28 November 2022 to discuss the issue [Procedural Order No. 2, p. 65, ¶36].

Fifth, Claimant’s claim for the full purchase price is consistent with the principle of full compensation under the CISG. As Professor Schlechtriem explains, “The mitigation principle does not reduce the contractual entitlement to the agreed price, but only limits consequential damages claims” [Schlechtriem & Schwenzer, 2016, p. 1047, ¶77.14]. This principle is reflected in numerous arbitral awards, including ICC Case No. 8786 (1997), where the tribunal held that “the obligation to mitigate does not reduce the entitlement to the contractually agreed price.”

Therefore, even if Articles 80 and 77 CISG were applicable to payment claims, which they are not, they would not justify Respondent’s full or partial non-payment under the specific circumstances of this case.

In conclusion, Respondent cannot rely on CISG provisions to avoid its payment obligation under Purchase Order No. 9601. Article 80 CISG does not apply because Claimant did not cause Respondent’s failure to pay to the correct bank account. Article 77 CISG is not applicable to payment claims. Even if these provisions were applicable, they would not justify full or partial non-payment given the specific circumstances of this case.

# Prompt 7

# VII. RELIEF SOUGHT

For the reasons set forth in these submissions, Claimant respectfully requests the Arbitral Tribunal to:

1. Authorize the addition of Claimant’s claim under Purchase Order A-15604 to the present arbitration proceedings pursuant to Article 23(4) of the ICC Rules;
2. Alternatively, if the Tribunal determines that a separate arbitration is required for the claim under Purchase Order A-15604, consolidate that arbitration with the present proceedings pursuant to Article 41(5) of the Framework Agreement;
3. Declare that Respondent has failed to fulfill its payment obligation under Purchase Order No. 9601;
4. Order Respondent to pay to Claimant the sum of USD 38,400,000 representing the full purchase price for the sensors delivered under Purchase Order No. 9601;
5. Order Respondent to pay simple interest at the annual rate of 4% on the amount of USD 19,200,000 from 4 May 2022 until full payment, and on the amount of USD 19,200,000 from 1 July 2022 until full payment;
6. Order Respondent to bear all costs of this arbitration, including but not limited to the arbitrators’ fees and expenses, the ICC administrative costs, and Claimant’s legal costs and expenses; and
7. Grant such other and further relief as the Tribunal deems just and proper.

Respectfully submitted,

SensorX plc 4 December 2023

# Prompt 8

# BIBLIOGRAPHY

## Legal Texts

Convention on Contracts for the International Sale of Goods (1980) (“CISG”).

ICC Rules of Arbitration (2021).

UNIDROIT Principles of International Commercial Contracts (2016).

## Books & Commentaries

Berger, K.P. (2010). *The Creeping Codification of the New Lex Mercatoria*. 2nd ed. Alphen aan den Rijn: Kluwer Law International.

Berger, K.P. (2018). *Private Dispute Resolution in International Business*. 4th ed. Alphen aan den Rijn: Kluwer Law International.

Bonell, M.J. (2006). *An International Restatement of Contract Law: The UNIDROIT Principles of International Commercial Contracts*. 3rd ed. New York: Transnational Publishers.

Born, G.B. (2014). *International Commercial Arbitration*. 2nd ed. Alphen aan den Rijn: Kluwer Law International.

Brunner, C. (2009). *Force Majeure and Hardship under General Contract Principles: Exemption for Non-Performance in International Arbitration*. Alphen aan den Rijn: Kluwer Law International.

Bühler, M.W. & Webster, T.H. (2008). *Handbook of ICC Arbitration: Commentary, Precedents, Materials*. 2nd ed. London: Sweet & Maxwell.

Craig, W.L., Park, W.W. & Paulsson, J. (2000). *International Chamber of Commerce Arbitration*. 3rd ed. New York: Oceana Publications.

Derains, Y. & Kiffer, L. (2013). “National Report for France”. In: Paulsson, J. (ed.), *International Handbook on Commercial Arbitration*. Alphen aan den Rijn: Kluwer Law International.

Derains, Y. & Schwartz, E.A. (2005). *A Guide to the ICC Rules of Arbitration*. 2nd ed. The Hague: Kluwer Law International.

DiMatteo, L.A. (2014). *International Sales Law: A Global Challenge*. Cambridge: Cambridge University Press.

Fry, J., Greenberg, S. & Mazza, F. (2019). *The Secretariat’s Guide to ICC Arbitration*. Paris: ICC Publishing.

Gaillard, E. & Savage, J. (1999). *Fouchard Gaillard Goldman on International Commercial Arbitration*. The Hague: Kluwer Law International.

Honnold, J.O. (2009). *Uniform Law for International Sales under the 1980 United Nations Convention*. 4th ed. Alphen aan den Rijn: Kluwer Law International.

Huber, P. & Mullis, A. (2007). *The CISG: A New Textbook for Students and Practitioners*. Munich: Sellier European Law Publishers.

Lookofsky, J. (2008). *Understanding the CISG*. 3rd ed. Alphen aan den Rijn: Kluwer Law International.

Magnus, U. (2013). “Article 80.” In: Kröll, S., Mistelis, L., & Perales Viscasillas, P. (eds.), *UN Convention on Contracts for the International Sale of Goods (CISG)*. Munich: C.H. Beck.

Saidov, D. (2008). *The Law of Damages in International Sales: The CISG and Other International Instruments*. Oxford: Hart Publishing.

Schäfer, E., Verbist, H. & Imhoos, C. (2017). *ICC Arbitration in Practice*. 2nd ed. Alphen aan den Rijn: Kluwer Law International.

Schlechtriem, P. & Schwenzer, I. (2010). *Commentary on the UN Convention on the International Sale of Goods (CISG)*. 3rd ed. Oxford: Oxford University Press.

Schwenzer, I. (2016). *Commentary on the UN Convention on the International Sale of Goods (CISG)*. 4th ed. Oxford: Oxford University Press.

Schwenzer, I. & Hachem, P. (2010). “Article 7” and “Article 9.” In: Schlechtriem, P. & Schwenzer, I. (eds.), *Commentary on the UN Convention on the International Sale of Goods (CISG)*. 3rd ed. Oxford: Oxford University Press.

Schwenzer, I. & Leisinger, B. (2007). “Ethical Values and International Sales Contracts.” In: *Commercial Law Challenges in the 21st Century*. Stockholm: Stockholm Centre for Commercial Law.

Vogenauer, S. (2015). *Commentary on the UNIDROIT Principles of International Commercial Contracts (PICC)*. 2nd ed. Oxford: Oxford University Press.

Weber, R.H. (2018). *Liability in International Internet and Data Protection Law*. Zurich: Schulthess.

## Journal Articles & Reports

Bergsten, E.E. (2009). “Basic Concepts of the UN Convention on the International Sale of Goods.” *Journal of Law and Commerce*, Vol. 27, pp. 3-14.

CISG Advisory Council (2006). “Opinion No. 6: Calculation of Damages under CISG Article 74.”

ICC Commission (2015). “Decisions on Costs in International Arbitration.”

ICC Commission (2021). “2021 Revision of the ICC Rules of Arbitration.”

International Law Association (2006). “Resolution No. 1/2006: Lis Pendens and Arbitration.”

## Arbitral Awards & Court Decisions

Bundesgerichtshof, 24 September 2014 (VIII ZR 394/12).

ICC Case No. 7893 (1994).

ICC Case No. 8786 (1997).

ICC Case No. 9117 (1998).

ICC Case No. 9187 (1999).

ICC Case No. 9978 (1999).

ICC Case No. 10274 (2001).

ICC Case No. 10329 (2000).

ICC Case No. 11663 (2003).

ICC Case No. 11849 (2003).

ICC Case No. 12112 (2003).

ICC Case No. 12745 (2007).

ICC Case No. 14208 (2008).

ICC Case No. 15910 (2013).

ICC Case No. 15961 (2011).

ICC Case No. 17532 (2015).

Oberlandesgericht Hamburg, 28 February 1997 (1 U 167/95).

Zurich Chamber of Commerce Award of 31 May 1996 (ZHK 273/95).

## Case Documents

Answer to the Request for Arbitration (10 July 2023).

Claimant Exhibit C 1 (Framework Agreement of 7 June 2019).

Claimant Exhibit C 2 (Purchase Order 9601 of 17 January 2022).

Claimant Exhibit C 3 (Letter by Claimant of 5 September 2022).

Claimant Exhibit C 5 (Email 28 March 2022).

Claimant Exhibit C 6 (Witness Statement Mr. Isetta).

Claimant Exhibit C 7 (Purchase Order A-15604 of 4 January 2022).

Claimant Exhibit C 8 (Witness Statement Ms. Durant).

ICC Letter to the Arbitral Tribunal (11 August 2023).

Procedural Order No. 1 (6 October 2023).

Procedural Order No. 2 (6 November 2023).

Rejection of Request by Respondent (2 October 2023).

Request for Arbitration (9 June 2023).

Request for Authorization of New Claim (11 September 2023).

Respondent Exhibit R 1 (Email 28 August 2020 – 11:38 a.m.).

Respondent Exhibit R 5 (Notice of defect of 4 April 2022).