LEGAL CHALLENGES IN INTERNATIONAL COMMERCIAL PAYMENTS WITH SPECIAL REFERENCE TO LETTERS OF CREDIT IN THE DIGITAL ECONOMY

by

Jenifer Theresa Antony S

ABSTRACT

International commercial payments make the world go round, and Letters of Credit (LCs) are at the heart of it all, trusted by buyers and sellers everywhere. They've been the gold standard for minimizing risk in global trade, mostly thanks to the rules laid out in UCP 600. But times are changing fast. As trade moves online, we're seeing everything shift: electronic documents, blockchain, fintech apps, digital banks. These new tools are great, but they're also bringing a whole bunch of legal headaches, think questions about how to validate electronic documents, worries about authentication, cybersecurity, privacy, fraud, cross-border disputes, and keeping up with a patchwork of regulations. This study dives into the legal maze surrounding Letters of Credit in today's digital economy, focusing on how international payments work now. It takes a hard look at big legal frameworks like UCP 600 and the UNCITRAL Model Law on Electronic Transferable Records (MLETR), plus Indian laws such as the Information Technology Act, FEMA, and various banking rules. The research spots some pretty serious gaps, showing that the current laws aren't quite keeping pace with new digital risks. In the end, it calls for smarter regulations and fresh policies, so we can better control digital LCs, resolve legal uncertainties across borders, and make international trade safer, faster, and more reliable. All that, with the goal of protecting the integrity of global payments, even as technology keeps changing the game.

Keywords: Letters of Credit, UCP 600, Digital economy, International Commercial Payments, FEMA

Indian Journal of Law and Jurisprudence | Licensed under Creative Commons — https://creativecommons.org/licenses/by/4.0/ | DOI: 10.5281/zenodo.23402007 | Title: Legal Challenges In International Commercial Payments With Special Reference To Letters Of Credit In The Digital Economy

CHAPTER-I
INTRODUCTION

1.1 Background of The Study

International commercial payments can be considered the backbone of cross-border trade, linking buyers and sellers from diverse countries. But international deals come with difficulties one doesn't see in local transactions, distance, different legal systems, exchange rates going up and down, political uncertainties, and tricky contract enforcement. Exporters want to know they'll get the payment before sending goods, but importers falter to pay upfront without seeing what they may be getting. That's where Letters of Credit come in, they've become a trusted tool to link this gap. A Letter of Credit is fundamentally an arrangement where a bank promises to pay as long as the seller presents the right documents needed. This gives exporters some security, but it also means following strict documentary rules. One key point to note is that the bank's promise is separate from the actual sales contract, and it's all about the paperwork, not the goods.

To keep things standard, the International Chamber of Commerce came up with the Uniform Customs and Practice for Documentary Credits (UCP 600), a sort of rulebook adopted universal since 2007. But the world has gone digital, now we arere seeing electronic records, digital bills of lading, e-signatures, and paperless banking. This shift leads to a big legal question whether rules designed for paper documents can handle the risks and realities of digital trade? The ICC tried to answer this with the eUCP Supplement for electronic document presentation, but these rules don't operate in a void. They have to work side-by-side with each country's laws on things like electronic records, transferable documents, banking and cybersecurity. So, differences in law can create hardship when disputes pop up across borders.

1.2 Statement of the Problem

Converting to digital Letters of Credit hurries things up, reduces paperwork, and generally makes life easier. But digital records bring their own risks, manipulation, hacking, system glitches. And just because a law accepts an electronic record doesn't mean it sorts out issues of transferability, proof, or authenticity.

UCP 600 and the eUCP set the rules when encompassed in the contract, but national laws still decide questions like what's actually a valid electronic document or who pays if something goes wrong. Since there's no complete harmony between these frameworks, traders and banks can be left guessing about their legal position.

1.3 Research Objectives

This study aims to:

1. Break down the international legal framework around Letters of Credit;
2. Analyse the working of UCP 600 and eUCP in the digital world;
3. Judge whether Indian laws really support electronic documents and cross-border payments;
4. Pinpoint legal challenges on electronic documents, cybersecurity, fraud, and jurisdiction; and
5. Suggest reforms for safer, clearer digital payments in international trade.

1.4 Research Questions

The main questions guiding this work are:

1. How well do UCP 600 and eUCP cover digital Letters of Credit?
2. Does Indian law (as it stands) truly support electronic trade documents?
3. What legal risks come from cyber-attacks, digital fraud, or clashing national laws?
4. What legal changes are needed to bring more certainty to digital Letters of Credit?

1.5 Research Methodology

This research uses doctrinal legal methods, digging into statutes, rules, and regulations (like UCP 600, eUCP, UNCITRAL guidelines, Indian laws) and supplementing those with books and academic papers about international trade and e-commerce. There's a comparative angle too: Singapore's approach to electronic transferable records gets examined. The focus is purely qualitative and analytical, this isn't a statistics-driven risk assessment.

1.6 Review of Literature

People who've dug into international commercial payments and documentary letters of credit tend to zero in on legal certainty, documentary compliance, and tech progress in global trade. Hamed Alavi (2016) goes deep into the legal nature and the actual laws behind letters of credit. Roberto Luis Frías García (2010) unpacks the autonomy principle, basically, the idea that the credit stands on its own, separate from whatever commercial contract sparked it. Mohd Hwaidi (2014) looks at how the English strict compliance rule meshes with the Uniform Customs and Practice for Documentary Credits (UCP), showing just how crucial getting the paperwork right is. On top of that, Caslav Pejovic (2017) takes on the messiness

with dodgy transport documents under the UCP, pointing out legal headaches around documentary fraud.

Now, with international trade shifting toward digital, researchers are worrying more about electronic documentation, cybersecurity, and whether the law actually recognizes digital trade tools. The OECD (2025) breaks down the move to paperless trade and the rocky road of digitizing trade documents. Jurij Lampič and Irene Ng dig into how the UNCITRAL Model Law on Electronic Transferable Records might help automate contracts and handle metadata—they're basically mapping out how legal frameworks fit digital records. Grzegorz Szyjewski (2023) chases down ways to keep digital copies safe, while Suhasini Verma, Keshav Kaushik, and Vidhisha Vyas (2022) underline the constant threat of cyberattacks alongside digital payments. Shubham Diwate goes even further, looking at how private international law can handle the protection of digital trades and transactions online. All these studies point to one thing: digital trade needs solid legal protection, smart tech security, and a ton of international cooperation.

The rules and regulations for digital trade and global payments owe a lot to UCP 600, eUCP, and the UNCITRAL Model Law on Electronic Transferable Records. These cover everything from documentary compliance to legal recognition of electronic records. In India, laws like the Foreign Exchange Management Act, 1999; the Information Technology Act, 2000; and the Digital Personal Data Protection Act, 2023, set the tone for foreign exchange, electronic records, cybersecurity, and data protection. Ketut Ngastawa and Johannes Ibrahim Kosasih (2025) take a close look at standard clauses in global trade contracts, stressing the importance of having strong agreements for cross-border business. But honestly, how documentary credit rules, e-docs, cybersecurity, and domestic regulations fit together still needs a closer look. That's what this study aims to tackle, picking apart the legal challenges that come with digitizing international payments and seeing if today's global and local laws handle them well enough.

IJLJ
ISSN: 2583-2794

CHAPTER-2

INTERNATIONAL LEGAL FRAMEWORK GOVERNING LETTERS OF CREDIT

2.1 Nature and the Functioning of Letters of Credit

Letters of Credit have become central in global trade, helping both buyers and sellers manage payment and delivery risks. Here's how it works: a buyer asks their bank to issue a credit in the seller's favour. If the seller presents documents that meet all the requirements, the bank has to pay, simple as that. The point is, the bank doesn't care if the goods are perfect; it only checks the documents. So, while it reassures sellers about payment, it doesn't guarantee the actual delivery or quality of the goods.[1]

2.2 Uniform Customs and Practice for Documentary Credits

UCP 600 (since July 2007) sets out the key rules for documentary credits with 39 articles. It's not law, but a contractual set of rules that parties explicitly adopt. Article 1 says where it applies. Article 4 establishes that credits stand apart from the underlying sales contract. Article 5 means banks focus on documents, not the goods themselves. Article 14 covers how banks check documents, and Article 16 sets out the steps when there's a problem with the documents[2].

These rules give structure to international banking, but digital transactions add new layers. How one present, review, and authenticate digital documents can be a whole different task compared to paper.

2.3 The Principle of Autonomy and The Principle of Strict Documentary Compliance

The "autonomy principle" means that the bank's payment obligation is independent from any disputes about the goods. If the seller's documents meet the requirements, the bank must pay, even if something goes wrong with the goods[3]. Sellers count on this independence; they don't want their payment delayed by outside disputes. Still, this principle doesn't override everything, fraud is the main exception. If there's evidence of fraud, a court might step in, but the outcome depends on the laws involved and the specific situation.

[1] 1. Hamed Alavi, Documentary Letters of Credit, Legal Nature and Sources of Law, 17 J. Legal Stud. 106, 106–21 (2016), https://doi.org/10.1515/jles-2016-0012.
[2] International Chamber of Commerce, Uniform Customs and Practice for Documentary Credits, ICC Publication No. 600 (2007).
[3] Roberto Luis Frías García, The Autonomy Principle of Letters of Credit, 3 Mexican L. Rev. (2010), https://doi.org/10.22201/iij.24485306e.2010.5.7747.

Banks follow the letter of the credit. Any serious mistake or missing element in the documents can get a payment refused, UCP 600's Article 14 sets out examination rules, and Article 16 covers what happens if there's a discrepancy[4]. Now, digitalisation makes things tricky. If a document is in the wrong file type, metadata's missing, or it can't be accessed, it could count as non-compliance[5]. So, credits involving electronic presentations need to spell out technical formats, methods of presentation, and other tech details up front.

2.4 eUCP and Electronic Presentations

The ICC rolled out the eUCP to handle electronic presentations alongside or instead of paper documents. Version 2.1, effective since July 2019, covers what counts as an electronic record, how to present them, how banks check them, what's considered original or a copy, how to handle data corruption, and what the refusal process looks like[6]. Importantly, eUCP only applies if the credit specifically says so. In other words, electronic presentation doesn't automatically mean eUCP rules kick in.

eUCP improves clarity around documentary credits in the digital world, but it doesn't solve every legal issue. Questions about electronic bills of lading, cybercrime, or cross-border enforcement of judgments still depend on national laws, which don't always line up.

— I J L J —
ISSN: 2583-2794

[4] International Chamber of Commerce, supra note 2.
[5] Mohd Hwaidi, The Story of the English Strict Compliance Principle in Letters of Credit and Its Consistency with the UCP, 29 J. Int'l Banking L. & Reg. 71, 71–81 (2014).
[6] Int'l Chamber of Com., Uniform Customs and Practice for Documentary Credits (UCP) — Supplement for Electronic Presentation (eUCP), Version 2.1 (ICC Pub. No. 823E, 2023).

CHAPTER-3
LEGAL CHALLENGES IN THE DIGITAL ECONOMY

3.1 Electronic Trade Documents and its Legal Recognition

Electronic trade documents sit at the center of paperless international business. Things like bills of lading, invoices, and insurance records often aren't printed anymore, they're created, sent, and stored electronically. But there's a big difference between regular electronic records and electronic records designed to be transferable[7]. When it comes to traditional paper documents, whoever lawfully holds the document often holds important related rights. Hand someone the paper, and one hand them the rights vested with it too. Electronic systems have to match that function, but with extra hurdles, they need to stop unauthorized copies and avoid disputes over who has control over the document.

The UNCITRAL Model Law on Electronic Transferable Records, attempts to solve this[8]. Its main ideas are pretty basic, to not treat electronic means differently just because they're digital, focus on functional equivalence, and keep things tech-neutral. In short, it sets out guidelines for electronic records that need to stand in for traditional, transferable documents. But this law isn't automatically applicable. UNCITRAL can adopt it, but for it to be of significance within a country, local lawmakers have to actually pass a law based on it[9].

3.2 Cybersecurity and Electronic Fraud

Digital transactions rely on electronic messaging systems, banks' IT infrastructure, and specialized document platforms. All these modernisations pave way to cyber threats like phishing, hacking, malware, compromised accounts, or unauthorized changes. Say someone tampers with an electronic shipping document, or quietly swaps out payment instructions, the loss can go undetected, leading to real money vanishing and chaos over who's responsible and liable[10].

---

[7] Organisation for Economic Co-operation and Development, The Digitalisation of Trade Documents and Processes: Going Paperless Today, Going Paperless Tomorrow, OECD Trade Pol'y Paper No. 297 (2025), https://doi.org/10.1787/64872f25-en.

[8] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Transferable Records (2017).

[9] Jurij Lampič & Irene Ng (Huang Ying), An Analysis on the Application of the UNCITRAL Model Law on Electronic Transferable Records on Contract Automation and Metadata, in Legal Challenges in the New Digital Age 45–65, https://doi.org/10.1163/9789004447417_005.

[10] Suhasini Verma et al., Mounting Cases of Cyber-Attacks and Digital Payment, in Cybersecurity Issues, Challenges, and Solutions in the Business World 59–80 (2023), https://doi.org/10.4018/978-1-6684-5827-3.ch005.

When things go ultimately wrong, the hard part is pinpointing where the breakdown or the mistake could have actually happened. Was it the bank's weak checks, the beneficiary's carelessness, a vulnerable platform, or some criminal outside the system? The rules in UCP 600 and eUCP help with some aspects of these digital credits, but they're not full-blown cybersecurity manuals[11]. Banks and traders cannot bank on them alone, they need strong technological safeguards, watertight contracts, and strict internal procedures. Measures like multi-factor authentication, encryption, restricted access, audit logs, identity checks, and incident response plans all can be of help, but only if set up and sustained properly, and only if they match up with what the law actually demands.

3.3 Data Integrity and Authentication

Electronic documents travel across the world in mere seconds, but their value comes down to trust between the parties and the bank. The bank must be able to recognize the exact record, pull it up in the right format, and verify it against the rules of the credit. Digital signatures and cryptographic checks can prove legitimacy[12]. But just because a document is authentic doesn't mean the facts inside are actually accurate. A genuine, unedited document could still be filled with errors, meanwhile, a forged but technically "valid" record could be used to scam someone.

eUCP's Article e12 covers what happens if an electronic record gets corrupted[13]. Still, tech fiascos or bickering about a document's authenticity can easily land in court. So, a good legal framework should spell out how to verify these documents, how long to keep them, and what to do when digital records go lost, missing or get scrambled.

3.4 Applicable Law and Jurisdiction

With International Letters of Credit, buyers, sellers, and banks could each be physically present in different countries. Digital platforms add even more layers. So when problems come up, a few big questions follow: Which court handles the case? Whose law applies? What legal system decides if an e-document is valid? And, can a decision in one country actually be enforced in another?

[11] Caslav Pejovic, Fraudulent Transport Documents Under the UCP: Controversies and Possible Solutions, 171 Poredbeno Pomorsko Pravo 19–34 (2017), https://doi.org/10.21857/94kl4cw1vm.
[12] Grzegorz Szyjewski, Securing Digital Copies of the Documents to Ensure Documents' Integrity, 26 Eur. Rsch. Stud. J. 718–26 (2023), https://doi.org/10.35808/ersj/3321.
[13] Int'l Chamber of Com., supra note 6, art. e12.

Don't assume that just referencing UCP 600 settles every jurisdiction or legal question. The rules help, but they aren't a catch-all. Parties need to set out clear contracts outlining which laws and courts apply. Arbitration gets used a lot, and it can offer a more neutral battleground, but its value depends on how broad the arbitration deal is and whether local law backs it up.

3.5 Liability for Digital Transactions, Data Protection and Regulatory Fragmentation

Digital documentary credits usually involve a cast of banks (issuing, confirming, nominated), the beneficiary, and possibly tech service providers. Everyone's role, and legal risk, depends on the contracts and the laws at play. When fraud happens, there's often a messy debate about who takes the hit. The bank might insist they followed the rules; the beneficiary might claim the bank botched authentication or let the documents fall into the wrong hands[14]. Letters of Credit rules don't answer every legal problem tied to negligence, fraud, or third-party tech failures. That's why contracts must be clear, they should spell out who does what, their duties, authentication, secure communication, system checks, keeping evidence, and reporting issues. These clauses be obliged to align with mandatory legal and regulatory banking requirements[15].

Digital transactions unavoidably encompass personal information, sensitive financials, or trade secrets. When this data crosses borders, a fresh set of challenges pops up, questions arise on who can legally access it, where can it be kept, how must it be protected, and how can it be moved safely? Each country has its own rules for data protection and cybersecurity. A system following the law in one place might need big changes to meet stricter rules elsewhere. This patchwork makes compliance expensive and messy, especially for banks and exporters. So, while international coordination is crucial, any push for uniform rules has to balance global best practices with what individual countries need.

IJLJ ISSN: 2583-2794

[14] Shubham Diwate, Evaluating Challenges in Protection of Digital Trade and Transactions Through Cyberspace in Perspective of Private International Law, Int'l J. Legal Rsch. & Analysis, vol. II, no. 7 (Dec. 2024).
[15] Ketut Ngastawa & Johannes Ibrahim Kosasih, Standard Clauses in International Trade Agreements, 6 Int'l J. Rsch. Publication & Revs. 1367–71 (2025), https://doi.org/10.55248/gengpi.6.0825.2902.

CHAPTER-4
INDIAN LEGAL FRAMEWORK AND COMPARATIVE ANALYSIS

4.1 The Foreign Exchange Management Act, 1999

The Foreign Exchange Management Act (FEMA) is the backbone of India's foreign exchange system[16]. It covers the nuts and bolts of foreign exchange dealings, including payments that come with imports and exports. When it comes to Letters of Credit, FEMA and its related rules are essential for managing cross-border payments and compliance[17]. But FEMA isn't the final word on how documentary credits work, or on whether digital trade documents are legally valid. one also has to consider UCP 600, eUCP, other laws, and the terms in the contracts.

4.2 The Information Technology Act, 2000

The legal recognition to electronic records and electronic signatures is given by Information Technology Act, 2000, it also outlines how certain cyber offenses should be handled[18]. This makes it fundamental to India's digital Letters of Credit, since those all count on on electronic records and e-signatures. But just because an e-record is recognized by law, that doesn't mean it always counts as a transferable instrument or meets every Letter of Credit's requirements. one has to look at three separate things like validity of the record; can its contents be used as evidence and whether does it have all the features of a legally transferable document. These are not always the same.

4.3 Singapore's Approach to Electronic Transferable Records

Singapore is worth looking at. In 2021, it changed its Electronic Transactions Act to follow the UNCITRAL Model Law on Electronic Transferable Records[19]. This lets businesses legally use e-records that do the same job as paper bills of lading, solving big problems around control and integrity in digital settings. Singapore's approach shows the benefits of laws aimed specifically at transferable e-records, instead of just leaning on generic e-commerce rules.

[16] Foreign Exchange Management Act, No. 42 of 1999, India Code (1999).
[17] EnterSlice, Overview of Letter of Credit Under FEMA Rules, https://enterslice.com/learning/overview-of-letter-of-credit-under-fema-rules/ (last visited Oct. 14, 2026).
[18] Information Technology Act, No. 21 of 2000, India Code (2000).
[19] Electronic Transactions Act 2010

India can learn that recognizing e-records isn't enough. The law needs to spell out rules about how control is established, how integrity is kept, how the records transfer, and how rival claims are avoided. Of course, Singapore's law doesn't apply in India by itself. It's just a useful comparison.

4.4 The Need for Harmonisation

International trade law mainly relies on a whole series of compilation of overlapping rules and standards. UCP 600 covers documentary credits when it is properly covered by the contract. eUCP develops those rules to handle electronic presentations. The Model Law on Electronic Transferable Records (MLETR) gives a template for local laws, and national laws fill in gaps on things like foreign exchange, digital signatures, cybersecurity, and data privacy[20].

These systems aren't substitutable, just associated. The big challenge is making sure they all work organized. For instance, a Letter of Credit might allow electronic presentations under eUCP, but some other dispute could hinge on whether the e-bill of lading is a valid transferable instrument under Indian law. India needs to check if its current rules really cover electronic transferable records, and, if not, what new laws or updates are required to make things clearer and easier to comprehend

4.5 Cross-Border Dispute Resolution

When parties fall out over a Letter of Credit, they might go to court or turn to arbitration, assuming they've agreed to it. The International Chamber of Commerce runs DOCDEX, a process for trade finance disputes that offers expert determinations under special rules[21]. DOCDEX isn't the same as arbitration or a court decision, it only has the weight the parties and the local law give it.

With digital transactions, divergences can come up around document authenticity, system crashes, inconsistent records, or cybercrime. Solving these cases frequently takes real expertise in both trade finance and handling digital evidence. So, contracts should nail down how disputes will be resolved, which law applies, and which court or arbitrator settles issues, while making sure no mandatory rights are lost.

[20] United Nations Commission on International Trade Law, supra note 7.
[21] International Chamber of Commerce, DOCDEX: Documentary Instruments Dispute Resolution Expertise, https://iccwbo.org/dispute-resolution/dispute-resolution-services/adr/docdex/ (last visited Oct. 14, 2026).

CHAPTER-5
FINDINGS, RECOMMENDATIONS AND CONCLUSION

5.1 Findings

Here are the main points:

First, UCP 600 is the backbone for Letters of Credit, but it doesn't answer every legal question about electronic transferable records or cybersecurity. Second, eUCP opens the door for electronic presentations, but only if it's specifically included in the credit, and it supplements UCP 600, it doesn't replace it. Third, it's crucial to isolate the idea of legally recognizing electronic records from recognizing electronic transferable instruments. Transferability requires reliable systems that guarantee control and protect record integrity.

Fourth, digital transactions make it easier for fraud, cyberattacks, data errors, disputes over what law applies, and fights over liability. These go beyond the standard rules for documentary credits. Fifth, India's legal framework includes FEMA and the Information Technology Act, 2000, but that doesn't mean everything's covered. Electronic transferable records, and how all these laws fit together, need a closer look. Last, Singapore's adoption of the MLETR-based system offers a solid example for India as it considers legal reforms.

5.2 Recommendations

A few things should happen:

First, India needs to shore up its legal recognition of electronic transferable records. The country should review how the UNCITRAL Model Law might fit, and think about new laws or tweaks that address control, integrity, and easy transfer. Second, banks and businesses should use eUCP when it makes sense. They should lay out clearly which rules apply, what version, what formats are accepted, and how presentations work.

Third, all and sundry needs to maximize cybersecurity. Banks and tech providers should make sure their security, authentication, access controls, encryption, logs, and incident plans, is up to the level of threats they face. Fourth, contracts about Letters of Credit need to pin down who's responsible for handling e-documents, securing authentication, dealing with system failures, and reporting suspected fraud. Fifth, India's regulators ought to promote legal harmonisation. That means keeping Indian standards up-to-date with international best practices for electronic trade documents.

Sixth, dispute resolution clauses matter more than ever. Contracts should state if disputes go to arbitration or follow special procedures like DOCDEX, including what legal

effect those decisions have. Seventh, more attention needs to go to preserving good records. Banks and traders should keep reliable logs of document handling, authentication, decisions to accept or refuse, and more, so there's a solid trail in case disputes flare up.

Any variations should respect applicable laws and not disturb the clear, documentary foundation that makes Letters of Credit work.

5.3 Conclusion

Letters of Credit continue to play a key role in global trade and businesses by reducing payment risks and offering structured, document-based certainty. UCP 600 sets the standard for these transactions, and eUCP extends that logic to digital documents. But moving from paper to digital introduces challenges that simple contractual banking rules can't solve by themselves. We have new legal headaches: Will courts recognize and enforce electronic documents? How do we stop or resolve electronic fraud? What about protecting sensitive data and pinning down liability when things go wrong, especially when players operate across many countries? India has laid a solid base, with FEMA and the Information Technology Act, for policing payments and digital transactions. Still, it's not clear that this legal structure meshes perfectly with the unique demands of digital trade documents and modern banking. Other countries, like Singapore, show that carefully crafted laws for electronic transferable records make a real difference. India should study these approaches and figure out what fits its own systems and needs.

Moving ahead, the goal line isn't just to go "paperless", it's to shape a system for international payments that's legally robust and technologically protected. Achieving harmonized legal frameworks, better cybersecurity, clear liability rules, and effective dispute settlement will help every person to have confidence in digital Letters of Credit, while keeping the key principles of autonomy, rule-based compliance, and payment certainty intact. At the end of the day, international trade relies on trust. If legal systems can manage to keep pace with technology, without weakening that trust, then digital Letters of Credit have a bright future.

IJLJ ISSN: 2583-2794

BIBLIOGRAPHY

1. Alavi, Hamed. "Documentary Letters of Credit, Legal Nature and Sources of Law." 17 Journal of Legal Studies 106–121 (2016).

2. Frías García, Roberto Luis. "The Autonomy Principle of Letters of Credit." Mexican Law Review (2010).

3. Hwaidi, Mohd. "The Story of the English Strict Compliance Principle in Letters of Credit and Its Consistency with the UCP." 29 Journal of International Banking Law and Regulation 71–81 (2014).

4. Lampič, Jurij, and Irene Ng. "An Analysis on the Application of the UNCITRAL Model Law on Electronic Transferable Records on Contract Automation and Metadata." In Legal Challenges in the New Digital Age, 45–65.

5. Pejovic, Caslav. "Fraudulent Transport Documents Under the UCP: Controversies and Possible Solutions." 171 Poredbeno Pomorsko Pravo 19–34 (2017).

6. Szyjewski, Grzegorz. "Securing Digital Copies of the Documents to Ensure Documents' Integrity." 26 European Research Studies Journal 718–726 (2023).

7. Diwate, Shubham. "Evaluating Challenges in Protection of Digital Trade and Transactions Through Cyberspace in Perspective of Private International Law." International Journal of Legal Research and Analysis, vol. II, no. 7 (2024).

8. Ngastawa, Ketut, and Johannes Ibrahim Kosasih. "Standard Clauses in International Trade Agreements." 6 International Journal of Research Publication and Reviews 1367–1371 (2025).

9. Verma, Suhasini, Keshav Kaushik, and Vidhisha Vyas. "Mounting Cases of Cyber-Attacks and Digital Payment." In Cybersecurity Issues, Challenges, and Solutions in the Business World, 59–80.

WEBLIOGRAPHY

1. EnterSlice. "Overview of Letter of Credit Under FEMA Rules." Available at: https://enterslice.com/learning/overview-of-letter-of-credit-under-fema-rules/

2. International Chamber of Commerce. "DOCDEX: Documentary Instruments Dispute Resolution Expertise." Available at: https://iccwbo.org/dispute-resolution/dispute-resolution-services/adr/docdex/

3. Organisation for Economic Co-operation and Development. The Digitalisation of Trade Documents and Processes: Going Paperless Today, Going Paperless Tomorrow. OECD Trade Policy Paper No. 297 (2025). Available at: https://doi.org/10.1787/64872f25-en.

REFERENCES

International Rules and Instruments

1. International Chamber of Commerce, Uniform Customs and Practice for Documentary Credits (UCP 600), ICC Publication No. 600 (2007).
2. International Chamber of Commerce, Supplement to the Uniform Customs and Practice for Documentary Credits for Electronic Presentation (eUCP), Version 2.1, ICC Publication No. 823E (2023).
3. United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Transferable Records (2017).

Indian Legislation

1. Foreign Exchange Management Act, No. 42 of 1999 (India).
2. Information Technology Act, No. 21 of 2000 (India).
3. Digital Personal Data Protection Act, No. 22 of 2023 (India).

Comparative Legislation

1. Electronic Transactions Act 2010 (Singapore), as amended.

Institutional Reports and Publications

1. Organisation for Economic Co-operation and Development, The Digitalisation of Trade Documents and Processes: Going Paperless Today, Going Paperless Tomorrow, OECD Trade Policy Paper No. 297 (2025).
2. International Chamber of Commerce, DOCDEX: Documentary Instruments Dispute Resolution Expertise.
3. International Chamber of Commerce, Uniform Customs and Practice for Documentary Credits (UCP 600).
4. International Chamber of Commerce, Supplement to the Uniform Customs and Practice for Documentary Credits for Electronic Presentation (eUCP), Version 2.1.
5. United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Transferable Records (2017).

IJLJ — ISSN: 2583-2794