The American Journal of Political Science Law and Criminology
ISSN 2693-0803 | Open Access

TYPE Original Research
PAGE NO. 65-70
DOI 10.37547/tajpslc/Volume07Issue03-11

Analysis of objective and subjective elements of the crime of document forgery, selling, or using forged documents

Sadullaev Jaxongir Djamshedovich

Independent researcher at Tashkent State University of Law, Uzbekistan

OPEN ACCESS

SUBMITTED 29 January 2025
ACCEPTED 28 February 2025
PUBLISHED 31 March 2025
VOLUME Vol.07 Issue03 2025

CITATION

Sadullaev Jaxongir Djamshedovich. (2025). Analysis of objective and subjective elements of the crime of document forgery, selling, or using forged documents. The American Journal of Political Science Law and Criminology, 7(03), 65–70.
https://doi.org/10.37547/tajpslc/Volume07Issue03-11

Abstract: Document forgery represents one of the most pervasive and multifaceted crimes across jurisdictions, affecting areas such as contract law, property rights, financial transactions, and public trust in government-issued records. This study analyzes the objective (actus reus) and subjective (mens rea) elements of document forgery, selling of forged documents, and using forged documents, drawing on an extensive body of international legal scholarship, case law, and statutory frameworks. We discuss the conceptual foundations of forgery, the delineation between material and intellectual falsification, the significance of intent to deceive, and the punishments enforced. The article also explores emerging forms of forgery in electronic domains (e.g., digital signatures, manipulated images, and cyber-facilitated document falsification) and explains the forensic methodologies used to detect and prosecute these offenses. Ultimately, we highlight that while the objective elements require a demonstrable alteration or creation of a false document with legal significance, the subjective elements demand specific intent or knowledge of falsity aimed at deceiving a targeted party. The implications for legislative policy, prosecutorial practice, and emerging technologies in crime detection are discussed at length, drawing upon dozens of referenced scholarly works and statutory provisions.

Keywords: Document forgery, criminal law, actus reus, mens rea, fraud, forgery detection, white-collar crime, digital forgery.

Introduction: Document forgery is a crime that transcends borders, legal traditions, and societal contexts. It occupies a central role in legal, financial, and

administrative systems, as documents are core instruments upon which trust and certainty are built. The act of forging a document—or using, distributing, or selling such forged documents—undermines public and private trust in the integrity of documentation, threatens property rights, and destabilizes economic transactions. Document forgery, in its broadest sense, involves an alteration, fabrication, or counterfeiting process intended to deceive a recipient about the genuineness or authenticity of the record.

Criminalization exist in many jurisdictions worldwide, whether under the label "forgery," "utterance of forged documents," or "falsification of documents." Despite differences in specific statutory wording, the crime generally requires two essential elements: (1) an objective or material element (actus reus) consisting of making, altering, or using a counterfeit document, and (2) a subjective element (mens rea) that reveals the perpetrator's intention to deceive.

Given the centrality of trust and authenticity in both analog and digital worlds, the phenomenon of document forgery has evolved rapidly alongside technological advancement. Cyber-forgery or electronic document manipulation—including forging digital signatures, falsifying financial records, or fabricating e-tickets—further complicates legal analysis and enforcement. Additionally, the advent of advanced imaging and AI-based manipulation techniques ("deepfakes") introduces new layers of complexity in proving or disproving the genuineness of electronically produced or stored documents.

Despite the ubiquity of document forgery statutes across jurisdictions, the precise delineation of objective and subjective elements remains the subject of substantial legal debate. This problem is magnified by the emergence of electronic and cyber-facilitated forgeries that test the limits of traditional legal definitions. The questions that arise include:

- **How do different jurisdictions define and interpret the physical (objective) act of document forgery, including the creation, alteration, selling, and usage of forged documents?**
- **What constitutes sufficient mens rea for criminal liability in forgery cases, especially when considering negligence, recklessness, or knowledge of falsity?**
- **How do emerging forms of technology challenge or expand traditional notions of forgery and the evidentiary requirements to prove it?**

Addressing these issues requires an expansive review of domestic and international sources, case law, and statutory interpretation, along with a robust theoretical framework to encompass both the classical and modern forms of forgery.

METHODS AND RESULTS

This research adopts a qualitative legal-study design, grounded in doctrinal analysis, comparative legal studies, and interdisciplinary approaches that integrate forensic science perspectives. The study systematically reviews legislative texts, international treaties, court decisions, and legal scholarship to ascertain how different jurisdictions conceptualize and operationalize both actus reus and mens rea in forgery. In line with well-established legal-research methodologies, we employ textual interpretation, case-law synthesis, and cross-jurisdictional comparisons.

A key finding from the literature and statutory documents is the broad conceptualization of forgery as an act of altering or creating a document with the purpose of misleading others into believing it is genuine. Despite variances in wording, the majority of criminal codes delineate two core categories:

1. **Material (Physical) Forgery**: Involves physically altering an existing document or creating a document that never existed (e.g., forging signatures, modifying textual content, or adding false seals or stamps).
2. **Intellectual Forgery (False Statements)**: Involves inserting false information into a legitimate document, typically without altering its physical form, such as a notary attesting to untrue statements in an otherwise valid deed [1].

Objective Elements (Actus Reus) The predominant theme in the statutes is that the accused must engage in either making or adapting a writing or document in a manner that leads to the misrepresentation of facts. For instance, forging a signature, changing dates, or tampering with official seals qualifies as the actus reus [11, 13].

- **Creating a Completely New, Fake Document**: The perpetrator produces a document de novo, claiming it to be from a legitimate source or authorized individual.
- **Material Alteration of an Existing Document**: The offender modifies an extant, originally valid document—e.g., adding text, changing amounts in a financial record, substituting pages—to create a false impression.

A common statutory requirement is that the forged document be capable of producing legal consequences, such as conferring rights, establishing obligations, or serving as valid evidence. Courts in multiple jurisdictions treat the capacity to affect legal relations or produce binding legal outcomes as a necessary element of the actus reus[3]. If a document is so obviously false that it

cannot mislead, some legal systems do not consider it a forgery, or they treat it as a lesser offense [1].

Many legislations punish not only the creation of a false document but also its distribution, sale, or usage. For instance, in Indonesian law, using a forged letter as if it were genuine is specifically penalized under Article 263(2)[5]. Under U.S. federal law, employing or transmitting forged documents through the mail can trigger mail fraud charges [6]. The notion of "utterance" of a forged document, inherited from common law, underscores that passing a forgery into commerce or legal proceedings is as criminal as crafting it.

- **Intellectual vs. Material Forgery**: Some statutes or doctrinal interpretations differentiate forging the physical aspects (material forgery) from providing false statements (intellectual forgery).
- **Complete vs. Partial Forgery**: A partial forgery is any alteration to an otherwise valid document. Complete forgery involves creating or substituting the entirety.
- **Private Documents vs. Official Documents**: Penalty enhancements typically exist for official or "authentic" documents (e.g., government-issued IDs, notarial deeds).

Subjective Elements (Mens Rea) The corpus of reviewed materials consistently emphasizes intent to deceive as a bedrock requirement. The perpetrator's subjective aim must be to lead another to believe in the document's authenticity. Courts generally require proof that the accused was aware the document was false and intended to use it to achieve some form of advantage or to cause harm.

For conviction, the prosecution must establish that the accused had knowledge that the document was falsified. If the individual acted under a genuine mistake or unwittingly used a forged document, criminal liability does not attach. However, certain presumptions may arise if the accused possessed the document under highly suspicious circumstances.

Most jurisdictions categorize forgery as a specific-intent crime requiring a deliberate aim to deceive or defraud. However, some systems allow a lesser standard if the legal text or case law equates reckless disregard of the truth with sufficient mens rea [7]. Yet, the majority stance remains that the offender must willfully produce or use the forged document with the knowledge of its falsity.

While motive is distinct from intent, financial or personal gain is the most common impetus behind forging documents, whether to obtain loans, commit identity theft, or facilitate real-estate fraud [8]. Notaries who authenticate forged deeds may do so for financial incentive or to facilitate a client's illegal objective.

Contemporary analyses show a marked increase in electronic document forgery. The forging of digital signatures, manipulations of PDF files, tampering with metadata, and creation of entirely fictitious documents using digital tools are recognized offenses. In corporate settings, forging financial statements or altering accounting entries can fall under the broad category of document forgery, especially if these statements create legal consequences or are used to mislead regulators, shareholders, or creditors. Enron and WorldCom scandals exemplify how false financial records constitute forgery and lead to fraud convictions for executives [9].

Digital manipulation of images—e.g., forging passports by substituting faces, or deepfake technology that replaces video evidence—poses novel challenges for legal classification. Although the objective act remains altering a "document" or "record," proving the forgery, especially at a high resolution, demands advanced forensic techniques. These new forms expand the definition of "document" to include electronic or digital media [3].

Notaries and legal professionals sometimes face criminal liability for negligent or willful involvement in verifying forged documents, especially in transactions like property sales. Courts may impose criminal sanctions if a notary attests to unverified or blatantly false signatures. However, accidental or negligent oversight often leads to disciplinary action rather than imprisonment, unless clear intent to participate in the forgery is established [11].

Across legal systems, punishments typically range from six months to multiple years of imprisonment for basic forgery offenses. Enhanced penalties apply if the forgery involves official documents, or results in substantial financial harm [12]. In the United States, forging documents to perpetrate mail fraud can lead to up to 20 years of imprisonment, and if financial institutions are victimized, the sentence may be more severe [6]. Fines and restitution orders are common, particularly for financially motivated forgeries in corporate environments.

From the collected data, it is clear that the objective act of forgery involves creating or altering a document in a manner capable of misleading, whereas the subjective element demands an intent to deceive or defraud. Variations include the distinction between material and intellectual forgery, the requirement that the forged document is capable of legal consequences, and the difference between direct and indirect intent. The

selling or using of forged documents carries the same level of culpability once knowledge of falsity is established. The rise of digital technology has expanded the scope of forgery, prompting legislative responses worldwide.

DISCUSSION

The definition of "document" has expanded beyond physical papers to include electronic records, digital images, and intangible forms of data. This broader conceptualization aligns with the modern digital environment where intangible forms have legal significance. For instance, certain courts treat emails, PDF contracts, or intangible digital signatures as "documents" under forgery statutes when they can serve as legal evidence or create binding obligations.

A consistent principle across legal systems is that the forged document must be one that could realistically deceive and produce legal effects. If a spurious document is so obviously false that no reasonable person would accept it, or if it pertains to trivial matters with no legal ramifications, some jurisdictions do not classify it as forgery. The rationale is rooted in the harm principle; the law aims to penalize conduct that significantly threatens legal certainty and public trust.

In many civil-law jurisdictions, "authentic documents" enjoy a presumption of authenticity and carry significant legal weight [10]. Forgery of these documents is punished more severely because they are deeply tied to governmental or official authority—such as deeds, birth certificates, or state-issued identity cards. Such intensification of penalties reflects the potential for severe harm when official documents are falsified.

The overarching consensus in criminal jurisprudence is that forgery is not a strict liability offense. It demands the presence of fraudulent intent—dolus—to mislead another party. This principle ensures that innocent mistakes in documentation, unintentional alterations, or typographical errors do not result in criminal sanctions [7].

In practice, the challenge often lies in discerning whether the accused possessed the requisite knowledge. For instance, a clerk who processes documents might not realize they are forged, but a deliberate effort to ignore obvious signs of falsification could constitute willful blindness. Courts in many jurisdictions have crafted "red flag" doctrines, where patterns of suspicious or inconsistent documentation can shift the burden of explanation to the user or possessor of the alleged forgery [13].

Debates persist about whether criminal liability for forgery should extend to grossly negligent behavior. Some argue that corporate contexts require broader accountability to deter executives from "turning a blind eye" to questionable documents [4]. However, the traditional approach is that mere negligence is insufficient for criminal forgery charges. Most statues require proof of knowledge or "reckless disregard" for the truth.

Legal scholars highlight that criminal liability extends not only to the "fabricator" but also to anyone who knowingly sells or uses the forged document. This chain of liability can involve multiple participants in a forgery ring—designers, distributors, middlemen, and ultimate end-users. For example, an individual who sells forged passports commits forgery by facilitating the circulation of such documents, even if they did not physically create them.

As with creation, distributing or using a forged document necessitates knowledge and intent. A buyer who is duped into purchasing a forged document without knowledge of its falsity typically lacks the mens rea required for forgery. Prosecutors thus concentrate on evidence that the user knew or had strong reasons to suspect the document was not genuine.

The digital realm compounds these issues, where forged e-tickets, digital receipts, or fraudulent software licenses can be disseminated globally with minimal risk of detection. Tracking the chain of custody for intangible or electronic documents requires sophisticated forensic and cybersecurity measures. The extraterritorial reach of the internet heightens the complexity, leading to calls for international cooperation in penalizing cyber-forgery [2].

Traditional handwriting analysis remains foundational for proving signature forgeries. Techniques such as hyperspectral imaging, scanning electron microscopes, and ink chemical analysis can reveal tampering. The adoption of advanced technologies can bolster prosecutorial evidence, especially in high-stakes white-collar crimes.

For electronic documents, metadata logs, revision histories, and server access records serve as crucial evidence. Investigators rely on digital forensic experts to reconstruct the chain of modifications and identify anomalies like abrupt changes in timestamps or overwriting of logs. The reliability of such data is contingent on system integrity; if hackers or insiders manipulate logs, the forensic process becomes more complex.

Proving intent beyond a reasonable doubt is often challenging. Circumstantial evidence—such as the defendant's financial predicament, suspicious communications, or repeated usage of forged

documents—plays a major role. Meanwhile, civil-law jurisdictions sometimes apply a combination of documentary evidence, witness testimony, and expert reports to form an "intime conviction" of the judge.

Given that document forgery is increasingly transnational (e.g., forging passports, forging shipping documents for international trade), global harmonization of legal standards becomes essential. Regional bodies like the European Union and international law enforcement agencies, including Interpol, are working on uniform guidelines to improve mutual legal assistance in forgery cases.

Preventive strategies focus on improved document security, such as embedding sophisticated security features in official documents or employing blockchain-based verification for high-value transactions. Financial institutions are adopting AI-driven detection systems to flag unusual patterns that may suggest manipulated financial records.

The liability of professionals (e.g., notaries, lawyers, corporate officers) who facilitate or fail to detect forgery is a recurring theme. Strengthening ethical codes, conducting continuous training, and applying stricter sanctions for willful blindness can deter complicity. Regulatory bodies may impose additional compliance requirements, particularly in sectors like real estate, finance, and corporate governance where fraudulent documentation is common.

The law must adapt to advanced forgery techniques. Cyber-forgery tests the boundaries of conventional legislative definitions, prompting amendments or new enactments focused on digital authenticity, data integrity, and heightened cybersecurity. Innovative technologies like AI-based forgery detection can assist enforcement but also raise concerns about privacy, data governance, and the reliability of algorithmic evidence.

CONCLUSION

This article demonstrates that the crime of document forgery fundamentally revolves around two essential components: (1) an objective element (actus reus), which involves creating or altering a document—either physically or digitally—capable of producing legal consequences, and (2) a subjective element (mens rea) that underscores intentionality and knowledge of falsity. Jurisdictions across the world, including Indonesia, the United States, and various European countries, exhibit remarkable consensus on these core elements, although nuances exist in how they classify and punish forgery.

Several dimensions of forgery emerged as particularly salient in contemporary contexts:

1. **Material vs. Intellectual Forgery**: While material forgery involves physical or digital alterations, intellectual forgery revolves around false attestation without changing the document's outward form.
2. **Cyber-Forgery and Electronic Manipulation**: Modern technology has broadened the scope of forgery to include forging digital signatures, tampering with electronic data, and employing AI-based deepfakes, necessitating advanced forensic measures.
3. **Chain of Liability**: Selling, distributing, or using a forged document, when accompanied by the requisite knowledge, is often penalized as severely as the act of creation.
4. **Enhanced Penalties for Official Documents**: Official, authentic, or government-issued documents carry more severe penalties due to their high level of trust and potential for public harm when falsified.
5. **Evidentiary Challenges**: Proving intent (knowledge of falsity) is often the most challenging aspect, requiring a combination of forensic analysis, circumstantial evidence, and expert testimony.

Practical Recommendations

1. **Legislative Reforms**: Continuous updates to penal codes or electronic transaction laws are vital to address digital forms of forgery effectively. Legislatures should clarify definitions of electronic documents and specify forensic standards for cyber-forgery.
2. **Enhanced Forensic Collaboration**: Cross-border cooperation among forensic experts, law enforcement, and legal practitioners is essential to combat international forgery rings. Standardization of digital evidence protocols can strengthen prosecutions.
3. **Professional Accountability**: Intensify training, oversight, and disciplinary measures for notaries, lawyers, and corporate officers to mitigate risks of complicity in forgery. Ethical guidelines should stress due diligence and verification.
4. **Public Awareness**: Governments and institutions could conduct public awareness campaigns on recognizing forged documents. Encouraging vigilance among consumers, bank officers, and real-estate agents can lower the success rate of forgery scams.
5. **Technological Innovations**: Adoption of blockchain-based ledgers for high-value documents (e.g., land registries, property deeds) and robust cryptographic signatures can deter forging attempts by providing traceable authenticity.

Directions for Future Research

Further research could explore the interface between AI-driven document generation (e.g., advanced textual deepfakes), judicial admissibility of algorithmic forensic

methods, and the implications for due process rights. Comparative empirical analyses of prosecutorial outcomes in forgery cases across multiple jurisdictions may shed light on best practices for deterrence, evidence gathering, and sentencing rationales. Additionally, the psychological and criminological underpinnings of forgers—particularly in corporate settings—remain ripe for interdisciplinary investigation.

In conclusion, the legal constructs of actus reus and mens rea continue to define the boundaries of document forgery crimes. Emerging technologies call for a refined approach that remains faithful to foundational legal principles while adapting to new modalities of deceit. As forgery has become more sophisticated and transnational, effective legal frameworks, investigative techniques, and cross-institutional collaboration are indispensable in preserving the integrity of written evidence and public trust.

REFERENCES

Sipayung, I. M., & Hasanah, U. (2024). Forgery of a will with due regard to civil and criminal law. International Asia of Law and Money Laundering, 3(2), 138–143. https://doi.org/10.59712/iaml.v3i2.100

Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., Daulay, P., Meifilina, A., Alamin, T., Fitriana, R., Sutomo, S., Sulton, A., Noor, I. L., Rozuli, A. I., & Hallatu, T. G. R. (2019). Cybercrime case as impact development of communication technology that troubling society. International Journal of Scientific & Technology Research, 8(9), 1224–1228.

Rusu, I. (2022). Forgery of documents under signature. Legal and Administrative Sciences in the New Millennium, 11(1), 11–20.

Benson, M. L. (1985). Denying the guilty mind: Accounting for involvement in a white-collar crime. Criminology, 23(4), 583–607

Dwipayanti, S., & Suwondo, D. (2023). Criminal responsibility for perpetrators of the crime of diploma forgery. Ratio Legis Journal, 2(3), 1367–1382.

Podgor, E. S. (1992). Mail fraud: Opening letters. South Carolina Law Review, 43(2), 223–272.

Nguyen, T. H., & Pontell, H. N. (2010). Mortgage origination fraud and the global economic crisis: A criminological analysis. Criminology & Public Policy, 9(3), 591–609.

Dalnial, H., Kamaluddin, A., Mohd-Sanusi, Z., & Khairuddin, K. S. (2014). Detecting fraudulent financial reporting through financial statement analysis. Journal of Advanced Management Science, 2(1), 17–22. https://doi.org/10.12720/joams.2.1.17-22

Amiram, D., Bozanic, Z., Cox, J. D., Dupont, Q., Karpoff, J. M., & Sloan, R. (2018). Financial reporting fraud and other forms of misconduct: A multidisciplinary review of the literature. Review of Accounting Studies, 23(4), 732–783. https://doi.org/10.1007/s11142-017-9435-x

Samosir, T., Harlina, I., & Akbar, F. M. (2022). The legal implications of forgery, sale, and purchase binding agreement by a notary public. Nationally Accredited Journal, 9(4), 438–450

Putri, E. P. H., & Soponyono, E. (2024). Criminal liability for perpetrators of falsifying online loan identity documents. International Journal of Social Science Research and Review, 7(6), 184–192. http://dx.doi.org/10.47814/ijssrr.v7i6.2164

Dwipayanti, S., & Suwondo, D. (2023). Criminal responsibility for perpetrators of the crime of diploma forgery. Ratio Legis Journal, 2(3), 1367–1382.

Hadi, K. A. A., & Paino, H. (2016). Legal perspectives towards forgery, fraud, and falsification of documents: Recent developments. Malaysian Accounting Review, 15(2), 93–109