



Mens Rea Proof Standards in Electronic Fraud Crimes in Indonesia

Aida Fauziah Nur^{1*}, Adi Mansar²

Magister Ilmu Hukum Universitas Muhammadiyah Sumatera Utara

Corresponding Author: Aida Fauziah Nur: aidafauzyahnur01@gmail.com

ARTICLE INFO

Keywords: *Mens Rea*,
Criminal Proof, Electronic
Fraud, Electronic Evidence,
Criminal Liability.

Received : 27, July

Revised : 20, August

Accepted: 25, September

©2026 Nur, Mansar (s): This
is an open-access article
distributed under the terms
of the [Creative Commons
Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

The development of information technology has encouraged the increase in electronic fraud crimes with different characteristics from conventional fraud, especially in the aspect of proving the *mens rea* element as the basis for criminal liability. This research aims to analyze the position of *mens rea* in Indonesian criminal law, examine the problems of proof in electronic fraud cases, and formulate a construction of evidentiary standards that are more adaptive to the development of digital technology. The research uses normative legal research methods with laws and regulations, conceptual, and case approaches. Legal materials are analyzed qualitatively through systematic and prescriptive interpretation of laws and regulations, doctrines, and court decisions. The results of the study show that Indonesia's positive law does not yet have normative parameters that specifically regulate the standard of proof of *mens rea* in the crime of electronic fraud, so the assessment still depends on the judge's interpretation of the available evidence. This condition has the potential to cause disparities in verdicts and reduce legal certainty. This study offers a reconstruction of evidentiary standards through the **digital behavioural indicators approach**, namely the assessment of intentional elements based on the digital behavior patterns of perpetrators built from the integration of electronic evidence, digital forensic results, expert testimony, and trial facts. This approach is expected to strengthen the consistency of evidence, increase legal certainty, and still ensure the protection of the rights of defendants in the Indonesian criminal justice system.

INTRODUCTION

Digital transformation has changed the patterns of people's interactions in various sectors of life, including trade, financial services, communications, and public services. The use of the internet, *financial technology*, *electronic commerce*, and digital payment systems has created economic efficiency while expanding the space for information technology-based crimes. One form of crime that has experienced a significant increase is electronic fraud, which is the act of obtaining unlawful profits through information manipulation, misuse of digital identity, electronic system engineering, and the use of electronic communication means to mislead victims. The cross-border character, anonymity of perpetrators, and the ever-evolving use of technology make electronic fraud one of the main challenges in modern criminal law enforcement (Nikkel, 2020).

The development of the *modus operandi* of electronic fraud shows that the perpetrator no longer relies on a direct relationship with the victim as conventional fraud. Crimes are committed through social media, marketplaces, messaging applications, electronic mail, fake websites (*phishing*), *social engineering*, and the use of artificial intelligence to create identities or communications that appear authentic. This complexity causes that it is not enough to prove a criminal act only focusing on the victim's loss or objective act (*actus reus*), but must also be able to prove the element of error (*mens rea*) as the basis for criminal liability. In criminal law, the existence of intention, knowledge, intentionality, or other forms of error is an essential element that distinguishes criminal acts from administrative errors, defaults, or ordinary transaction failures (Collins, 2026).

In the Indonesian criminal law system, proving the element of guilt in the crime of electronic fraud still faces various normative problems. The new Criminal Code through Law Number 1 of 2023 still places the principle of *geen strafzonder schuld* as the foundation of criminal responsibility. On the other hand, regulations regarding criminal acts using electronic systems are spread out in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions along with various other sectoral provisions. However, the legislation does not provide comprehensive parameters regarding the standards of *proof of mens rea* in electronic fraud, especially in cases involving anonymous digital identities, the use of third-party accounts, automated transactions, or the involvement of various actors in a series of cybercrimes. As a result, proving the element of intentionality is often highly dependent on the interpretation of law enforcement officials and the judge's assessment of the digital evidence presented at trial (Wiarti, 2024).

This problem is increasingly complex because electronic evidence in essence describes more digital activities than the inner condition of the perpetrator when committing a criminal act. System activity logs, electronic communication history, IP addresses, metadata, and transaction track records can indicate a person's involvement in an event, but it does not automatically prove the intent to commit fraud. In judicial practice, this situation poses a challenge in drawing a logical relationship between digital evidence and

intentional elements, especially when the perpetrator denies his knowledge or criminal purpose. Therefore, proof of *mens rea* in electronic fraud requires an approach that relies not only on direct evidence, but also on an assessment of the set of facts, patterns of behavior, and the interconnectedness of the evidence that shape the judge's beliefs (Farah Farिकासari Firjatullah Faqih, 2026).

At the international level, the development of cyber law shows a tendency to develop a more adaptive approach to the characteristics of digital crime. Various court decisions in a number of jurisdictions accept the use of *circumstantial digital evidence* as a basis for concluding the existence of knowledge, intent, or intention, as long as the relationship between proven facts and conclusions regarding *mens rea* is rationally established and meets the standard of proof in criminal law. These developments show that proving subjective elements in cybercrime requires a different legal construction from conventional crimes due to the nature of the crime that takes place in the digital environment.

Previous research has generally focused on proving electronic evidence, the validity of digital evidence, or the effectiveness of law enforcement against cybercrime. Studies on electronic fraud also focus more on aspects of victim protection, *modus operandi*, and the implementation of the Electronic Information and Transaction Law. Meanwhile, research that specifically analyzes *mens rea* evidentiary standards as a subjective element of electronic fraud crimes in the perspective of Indonesian criminal law is still relatively limited. There have not been many studies that integrate error theory, criminal proof standards, characteristics of digital evidence, and the development of cyber law to formulate *mens rea proof parameters* that are able to provide legal certainty without reducing the protection of the rights of the defendant (Adi Mansar, Rai Rake Setyawan Rai Rake Setyawan, Vania Micha Dwilizadi Vania Micha Dwilizadi, Duma Indah Sari Lubis, 2026).

Based on these gaps, this study offers novelty in the form of a reconstruction of *mens rea evidentiary standards* in electronic fraud crimes through an integrated approach between criminal liability theory, evidentiary law, and the characteristics of digital evidence. This study not only evaluates the adequacy of Indonesia's positive legal arrangements, but also develops an analytical framework regarding indicators that can be used by judges in concluding the existence of intentional elements based on electronic evidence in a rational, proportionate manner, and still guaranteeing the principle of presumption of innocence.

This study aims to analyze the legal arrangements regarding *mens rea* proof in electronic fraud crimes in Indonesia, identify normative problems that arise in evidentiary practice, and formulate the construction of proof standards that are more adaptive to the development of digital technology while still based on the principles of legal certainty, justice, and human rights protection in the criminal justice system (Erwin Asmadi, Adi Mansar, Triono Eddy, Mukti Fajar Nur Dewata, Farid Wajdi, 2024).

THEORETICAL REVIEW

Theory of Error

The theory of guilt is one of the fundamental theories in criminal law that explains that a punishment can only be imposed if the perpetrator is not only proven to have committed an act prohibited by law, but also proven to have a mistake as the basis for criminal responsibility. This theory departs from the principle of *geen straf zonder schuld* which affirms that there is no crime without mistakes. Thus, guilt becomes the element that connects the criminal act with the responsibility of the perpetrator, so that punishment is not solely based on the consequences caused, but also on the existence of a reprehensible inner attitude when the act is committed (Arief, 2018).

According to Barda Nawawi Arief, mistakes are the normative basis for criminal responsibility which must be proven through the fulfillment of several elements, namely the ability to be responsible, the existence of a form of mistake in the form of intentionality or forgetfulness, and the absence of a reason that eliminates error. Therefore, proving guilt is not only directed at proving that the perpetrator committed an act, but also to ensure that the perpetrator has a psychological relationship with the act so that it is juridically worthy of criminal responsibility. This approach shows that Indonesian criminal law does not adhere to strict *liability* as a general principle, but still places guilt as the main condition of punishment (Arief, 2008).

In the context of electronic fraud crimes, the theory of error is very important because the element of intentionality generally cannot be proven directly. The perpetrators' activities are more recorded in the form of electronic data, digital transaction history, communication through electronic media, and the use of certain digital identities. Therefore, the existence of a mistake must be inferred through a logical relationship between the facts revealed and the behavior of the perpetrator before, during, and after the crime was committed. Thus, the theory of error is used in this study as a basis to analyze whether the electronic evidence submitted at trial has been able to prove the existence of an element of intentionality as the basis for criminal liability in the crime of electronic fraud.

Proof Theory

The theory of proof explains that the evidentiary process is a stage that determines whether or not there is criminal liability for a person. Proof not only serves to prove that a criminal act has really occurred, but also to prove all elements of the criminal act as formulated in the criminal provisions, including subjective elements in the form of the perpetrator's fault. Therefore, the standard of proof is an instrument that determines whether the evidence submitted has sufficient power to form the judge's confidence in passing a verdict (Harahap, 2016).

According to M. Yahya Harahap, proof in Indonesian criminal procedure law is a process to obtain the judge's conviction based on valid evidence as determined by law. The evidentiary system adopted by the Criminal Code requires a balance between normative provisions regarding evidence and the judge's beliefs, so that criminal verdicts cannot be based solely on personal beliefs

or only on the formal existence of evidence. The judge must assess the relevance of each piece of evidence as a whole so that a logical and objective construction of evidence is formed, and able to explain all elements of the criminal act charged.

The development of information technology presents new challenges in the evidentiary process, especially when criminal acts are committed through electronic systems. Digital evidence generally only shows electronic activity, while the element of intentionality as part of the error is not explicitly visible in the data. Therefore, the judge is required to conduct a comprehensive assessment of the relationship between electronic evidence, witness statements, expert testimony, clues, and other facts revealed at the trial to conclude that there is an element of intentionality. In this study, the theory of proof is used as a basis to evaluate whether the criminal proof system in Indonesia has adequate standards in proving *mens rea* in the crime of electronic fraud, as well as as a basis for formulating proof parameters that are more adaptive to the characteristics of information technology-based crimes.

METHODOLOGY

The method used in this study is *normative legal research* which aims to examine the legal construction of the standard of proof of *mens rea* elements in the crime of electronic fraud. This research starts from the view that law is a set of norms that are systematically arranged through laws and regulations, legal principles, doctrines, and court decisions that are the basis for determining criminal liability. With this perspective, the study is focused on examining the legal norms that govern the proof of the element of error, including assessing the level of harmony between regulations, the adequacy of their regulation, and their relevance in dealing with the characteristics of criminal acts committed through electronic media. The analysis was carried out to obtain juridical arguments regarding *mens rea* evidentiary standards that are able to provide legal certainty while ensuring the application of proportional criminal liability in the Indonesian criminal justice system.

RESULTS AND DISCUSSION

The Position of Mens Rea as the Basis for Criminal Liability in Determining the Crime of Fraud Based on Indonesian Criminal Law

The Indonesian criminal law system places mistakes as the main foundation in determining whether or not a person can be held criminally responsible. Consequently, the proof of a criminal act does not stop at proving the existence of an act that meets the formulation of delicacy, but must be continued with proof of the psychological relationship between the perpetrator and the act he committed. This relationship is known as *mens rea*, which is an inner state that indicates intentionality, knowledge, or other forms of wrongdoing required by criminal law. Without proof of this element, the punishment will lose its juridical legitimacy because it is contrary to the principle of *geen straf zonder schuld*, which has long been a fundamental principle in the Indonesian criminal accountability system (Nasution, 2025).

In the perspective of national criminal law, the existence of *mens rea* is not always explicitly stated in every formulation of a criminal act, but its existence can be traced through the use of terms that indicate the existence of an element of intentionality, such as "with intent", "deliberately", "knowing", or "unlawfully". Such a formulation shows that the lawmaker not only requires proof of the physical act of the perpetrator (*actus reus*), but also requires proof of the mental attitude behind the action. Therefore, *mens rea* is not just a complementary element, but a parameter that determines whether an act can be qualified as a criminal act that gives rise to criminal liability (Njoto, 2024).

This construction is also reflected in Law Number 1 of 2023 concerning the Criminal Code, which emphasizes that punishment can only be imposed on people who commit criminal acts by mistake, except in certain circumstances expressly specified by law. The regulation shows that Indonesian criminal law still maintains the principle of fault as the basis for criminal liability while limiting the possibility of applying strict *liability* only to certain offenses that are regulated in a limited manner. Thus, *proof of mens rea* remains an essential requirement in fraud cases, including fraud committed through electronic media (Dhimas Abie Thoyib, Adi Mansar, 2026).

In criminal acts, the *element of mens rea* fraud has different characteristics from other material crimes. Fraud is essentially a crime built through the process of creating false beliefs, manipulating the victim's perception, and encouraging the victim to voluntarily give up property based on misleading information. Therefore, the subjective element in the form of an intention to obtain profits illegally has emerged from the early stages when the perpetrator designs a fraudulent scheme. In other words, actions such as the use of false identities, the delivery of false information, the impersonation of digital accounts, or the engineering of electronic communications are not just a series of technical acts, but are manifestations of intentional mislead the victim (Syukur, 2015).

The existence of *mens rea* in the criminal act of fraud also distinguishes criminal acts from civil disputes, defaults, or business transaction failures. Not every loss that arises in a legal relationship can be qualified as a criminal act of fraud. The distinguishing element lies in the intention from the beginning to commit deception or provide false information to obtain profits that are contrary to the law. If the intention cannot be proven, then the settlement of the dispute is more appropriate to be placed in the realm of civil law. Therefore, *mens rea proof* serves as an instrument that maintains the boundary between legitimate criminalization and excessive criminalization of private legal relationships.

The complexity of proof increases when fraud is carried out through electronic systems. The perpetrator's activities are generally represented in the form of digital footprints, such as metadata, access logs, electronic transaction history, communication through instant messaging applications, the use of IP addresses, and other digital evidence. The evidence basically only shows the existence of electronic activities and has not directly described the inner state of the perpetrator. Therefore, the judge cannot conclude the existence of *mens rea* based solely on the existence of electronic transactions or the use of a digital

account, but must assess the entire set of facts that show the existence of a pattern of actions that logically lead to intentional fraud.

In the practice of proof *mens rea* in the criminal act of electronic fraud, it is more accurately understood as the result of the process of legal inference. The conclusion about the existence of intentionality is built through the relationship between various corroborating evidence, such as communication patterns with the victim, the timing of the transaction, the use of fictitious identities, the systematic transfer of funds, and the actions of the perpetrator after obtaining profits. This approach shows that *proof of mens rea* does not depend on the confession of the perpetrator, but on the judge's ability to construct a logical relationship between the proven facts and the elements of guilt required by law.

Based on this analysis, the *position of mens rea* in Indonesian criminal law not only functions as a condition for criminal accountability, but also as an instrument to ensure the application of the principles of justice, legal certainty, and proportionality in law enforcement. In the case of electronic fraud, the proof of the element of intentionality must be placed as the core of the examination because it is the basis for distinguishing between perpetrators who consciously design criminal acts and parties who are simply involved in an electronic transaction without having the will to commit fraud. Therefore, the development of *mens rea* evidentiary standards that are able to accommodate the characteristics of digital evidence is an urgent need in the reform of Indonesia's criminal law so that law enforcement against cybercrime continues to uphold the principle of fair criminal accountability.

Proof of Mens Rea in the Case of Electronic Fraud in Indonesia

Proof of *mens rea* is one of the most complex aspects in handling electronic fraud crimes. In contrast to objective elements that can be observed through the existence of actions, consequences, and causal relationships, *mens rea* is related to the inner state of the perpetrator that cannot be seen directly. Therefore, the evidentiary process is not directed to find evidence about the contents of the perpetrator's mind, but rather to build legal conviction about the existence of intentionality based on a series of facts proven at trial. Thus, *mens rea proof* is a process of juridical reasoning (*legal reasoning*) that connects evidence with inference about the existence of a will to commit fraud (Tubagus Ahmad Ramadan, 2025).

In the Indonesian criminal proof system, the existence of *mens rea* cannot be separated from the provisions of Article 183 and Article 184 of the Criminal Procedure Code (KUHAP). Article 183 of the Criminal Code requires that a judge can only impose a criminal sentence if he obtains a conviction based on at least two valid evidence that a criminal act actually occurred and that the defendant is the perpetrator. This provision shows that the judge's conviction should not be built on mere suspicion, but must rely on a logical relationship between the evidence and all elements of the criminal act, including the element of intentionality. In other words, *proof of mens rea* is not a stand-alone proof, but an integral part of proving

all elements of delicacy (Gusti Muhammad Andre, Barda Nawawi Arief, RB Sularto, Faiqah Nur Azizah, 2025).

The characteristics of the crime of electronic fraud cause *proof of mens rea* to have a higher level of difficulty than conventional fraud. Perpetrators generally take advantage of fake digital identities, bank accounts belonging to other parties, prepaid phone numbers, anonymous social media accounts, *virtual private networks* (VPNs), or electronic payment systems that make it difficult to identify the relationship between the perpetrator and the digital activity carried out. On the other hand, most interactions between perpetrators and victims take place through electronic media without any physical encounters. This condition causes the inner state of the perpetrator cannot be deduced from just one type of evidence, but must be analyzed through a whole series of digital activities that show the existence of a pattern of planned actions (Siregar, 2019).

In the practice of proof, the *element of mens rea* in the crime of electronic fraud is more built through *circumstantial evidence*. This approach does not mean lowering the standard of proof, but is a logical consequence of the character of digital crimes that leave an electronic footprint rather than evidence of the perpetrator's intentions. For example, the repeated use of fictitious identities, the creation of special accounts to commit fraud, communications that systematically contain false information, the transfer of funds to various accounts in a short period of time, the deletion of data after a successful transaction, and the termination of all communication access with the victim after obtaining profits. These facts, when interrelated and corroborated by other evidence, can form a rational inference about the intentionality of fraud.

Electronic evidence has an important position in proving the crime of electronic fraud as recognized in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. Electronic Information, Electronic Documents, and their printed results are valid legal evidence as long as they are obtained and processed in accordance with the provisions of laws and regulations. However, the existence of electronic evidence does not necessarily prove the existence of *mens rea*. The evidence only shows the existence of digital activities, while proving the element of intentionality still requires an evaluation process of the context, the purpose of using electronic media, communication patterns, and the relationship between the perpetrator's actions and the losses experienced by the victim (Ayu Rahmania, M. Faisal Dio Azhary, 2025).

From the perspective of evidentiary law, the judge is required to conduct a holistic assessment of all evidence submitted at trial. Witness statements, digital forensic expert statements, letters or electronic documents, instructions, and the defendant's statement should not be assessed separately, but must be placed as a complementary unit. Such an approach is important to avoid conclusions that are based solely on the existence of a recipient's account or the ownership of a particular electronic account without any evidence of the active involvement and intent of the perpetrator in carrying out the fraudulent scheme (Wahyu Sabrudin, Triono Eddy, 2024). Thus, *proof of mens rea* must be built through a logical

relationship between the evidence and the defendant's behavior before, during, and after the criminal act was committed.

Another problem that is still found in judicial practice is the absence of normative parameters that clearly regulate *indicators of proof of mens rea* in information technology-based crimes. As a result, there are variations in the judge's consideration when assessing the element of intentionality. In certain cases, the existence of electronic communications and the transfer of funds is considered sufficient to prove malicious intent, while in other cases the judge requires additional evidence showing the defendant's active involvement in the entire fraud series. These differences in approach have the potential to cause disparities in verdicts, even though legal certainty requires a consistent standard of proof for cases with similar characteristics.

According to the author, *the standard of proof of mens rea* in the crime of electronic fraud should not only rely on the existence of electronic evidence, but also on *behavioral indicators* that show the intention to commit fraud. These indicators can be in the form of intentional use of false identities, planning fraud schemes, mastering the proceeds of crime, hiding digital traces, coordination with other perpetrators, and actions that are consciously carried out to avoid tracking by law enforcement officials. This approach is more in line with the principle of criminal liability because the conclusion about *mens rea* is built through a thorough evaluation of a series of facts, rather than solely based on one specific piece of evidence.

Therefore, *proof of mens rea* in electronic fraud cases requires a reconstruction of evidentiary standards that are able to integrate criminal procedure law with the development of digital technology. The standard should provide clearer guidelines regarding the relationship between electronic evidence, indirect digital evidence, and judges' reasoning in inferring the element of intentionality. With more measurable parameters, the evidentiary process not only increases the effectiveness of law enforcement against perpetrators of electronic fraud, but also ensures the protection of the rights of defendants through the application of the principles of presumption of innocence, legal certainty, and fair justice.

Obstacles and Solutions for Mens Rea Proof in Electronic Fraud Cases in Indonesia

The development of information technology has changed the character of fraud crimes from crimes that were originally committed through direct interaction to crimes that take place in the digital space. These changes not only affect the modus operandi of the perpetrator, but also present new challenges in the evidentiary process, especially with regard to the elements *Mens Rea* as the basis for criminal liability. If in conventional fraud the perpetrator's intentions can be traced through behavior, communication, or direct contact with the victim, then in electronic fraud the relationship is often represented in the form of digital traces that are not always able to describe the perpetrator's inner state explicitly. As a result, the proof *Mens Rea* is one of the most difficult aspects in the examination of electronic fraud cases in Indonesia (Dennis Fernando, Dini Dewi Heniarti, 2025).

Based on an analysis of legal regulations and law enforcement practices, there are several main obstacles in proving *mens rea* in electronic fraud crimes in Indonesia, namely (Erwin Asmadi, Adi Mansar, 2023):

1. There is no normative parameter regarding *mens rea* proof
Laws and regulations in Indonesia, both Law Number 1 of 2023 concerning the Criminal Code and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, have not provided guidelines that specifically regulate indicators of proof of *the element of mens rea* in information technology-based crimes. As a result, the assessment of the element of intentionality is still highly dependent on the interpretation of the judge, so that it has the potential to cause disparity in decisions in cases that have similar characteristics.
2. Characteristics of digital evidence that do not directly reflect the inner state of the perpetrator
Electronic information, metadata, system logs, IP addresses, transaction history, and digital communications only indicate the existence of electronic activity, but cannot directly prove the intention or intent to commit fraud. This condition causes the judge to make inferences from various available evidence to ensure that there is a relationship between digital activities and elements of error.
3. Use of an anonymous or loaned digital identity
In the practice of electronic fraud, perpetrators often use bank accounts belonging to other people, fake social media accounts, prepaid phone numbers, identity *theft*, and electronic devices that do not belong to them. Therefore, the ownership of an account or account is not always identical to the perpetrator of a criminal act so that *proof of mens rea* cannot be based solely on the digital identity used.
4. The complexity of organized and cross-jurisdictional crimes
Electronic fraud generally involves several perpetrators with different roles sharing, such as fake website creators, communication operators with victims, shelter account providers, and parties in charge of moving the proceeds of crime. This condition causes the proof of the element of intentionality to be carried out individually against each perpetrator based on his contribution to the entire series of criminal acts.
5. Limited capacity of law enforcement officials in digital proof
Not all investigators, public prosecutors, and judges have adequate competence in understanding the characteristics of electronic evidence and the results of digital forensic examinations. Weaknesses in the process of confiscation, securing evidence, *digital forensic acquisition*, and maintaining the *chain of custody* can reduce the evidentiary value of electronic evidence in trial.

According to the author, these various obstacles show that the main problem of *mens rea* proof does not lie in the lack of electronic evidence, but in the absence of juridical standards that are able to connect digital evidence with

intentional elements objectively and measurably. So far, the assessment of *mens rea* is still highly dependent on the judges' beliefs built from their respective interpretations of the facts of the trial. Such conditions are indeed in line with the evidentiary system according to the Criminal Code, but in cybercrime cases, more specific parameters are needed so that the space for subjectivity in assessing the element of error can be minimized. In other words, the reform of evidentiary law should be directed not at diminishing the independence of judges, but at providing guidelines capable of producing more consistent verdicts.

To overcome various obstacles in proving *mens rea* in electronic fraud crimes, updates are needed both in terms of regulations and law enforcement practices. The solutions that can be done are as follows:

1. Reconstructing the standards of proof of *mens rea* through judicial guidelines

The Supreme Court needs to develop guidelines that specifically regulate the parameters of proof of *the mens rea element* in electronic fraud cases, both through the Supreme Court Regulation (PERMA) and the Supreme Court Circular Letter (SEMA). The guidelines should contain objective indicators that can be used as a reference for judges in assessing the presence of intentional elements based on electronic evidence, so that the evidentiary process does not only depend on individual interpretation. The existence of this guideline is expected to be able to reduce disparity in verdicts while increasing legal certainty and consistency in the application of criminal law.

2. Applying an integrated evidentiary approach based on evidence integration

Mens rea proof should not be based on one type of evidence, but rather built through mutually reinforcing relationships between various available evidence. Electronic communication patterns, transaction chronology, use of digital identities, flow of funds, results of digital forensic examinations, expert testimony, and defendants' behavior before and after the crime was committed must be analyzed in an integrated manner. This approach allows judges to build more rational inferences about intentionality, while remaining in line with the evidentiary system according to the Criminal Code.

3. Increasing the capacity of law enforcement officials in the field of digital proof

Investigators, public prosecutors, judges, and digital forensic experts need to continuously strengthen their competencies regarding electronic evidence examination techniques, digital data analysis, *digital forensics*, and information technology developments. This capacity building is important so that each electronic evidence can be assessed appropriately, both in terms of validity and relevance in proving the element of error. Uniformity of understanding between law enforcement will also reduce differences in interpretation in the evidentiary process.

4. Strengthening inter-agency and cross-border cooperation in the search for digital evidence

The cross-jurisdictional nature of electronic fraud requires more effective coordination between law enforcement officials and electronic system operators, banking institutions, telecommunication service providers, financial services authorities, and law enforcement agencies in other countries. This synergy is needed to accelerate the tracking of the identity of the perpetrator, secure digital traces, trace the flow of funds, and obtain electronic evidence outside the jurisdiction of Indonesia.

According to the authors, the update of *the mens rea evidentiary standard* in the criminal act of electronic fraud must be placed as part of the reform of the criminal procedure law in the digital era. The law of proof is no longer enough to regulate the type of evidence that can be used, but it is also necessary to provide guidelines regarding the judge's reasoning method in connecting digital evidence with the element of error. With this reconstruction, the evidentiary process will be more adaptive to technological developments, reduce disparities in verdicts, increase legal certainty, and still ensure the protection of the human rights of defendants through the application of the principle of presumption of innocence and the principles of fair justice. The novelty offered by this study lies in the formulation of *mens rea* proof standards based on digital *behavioural indicators*, so that the proof of intentionality does not only depend on the existence of electronic evidence, but also on a systematic analysis of the actor's action patterns, goals, and series of digital activities as a unit that forms the judge's beliefs.

CONCLUSIONS AND RECOMMENDATIONS

Mens rea has a fundamental position as the basis for criminal liability in the crime of electronic fraud in Indonesia because it is an element that connects unlawful acts with the fault of the perpetrator. Proof of this element cannot only be based on the victim's loss or the existence of electronic evidence, but must be able to show the will, knowledge, or purpose of the perpetrator to obtain unlawful profits. Therefore, *proof of mens rea* must be understood as a process of legal reasoning that is built through a logical relationship between the facts revealed at trial and the element of intentionality as required in Indonesian criminal law.

This study found that Indonesia's positive legal regulation has not provided normative standards that specifically regulate the parameters of *mens rea proof* in electronic fraud cases. Although the Criminal Procedure Code has regulated the evidentiary system and the Electronic Information and Transaction Law has recognized electronic evidence as valid evidence, there are no guidelines on how to connect digital evidence with the subjective elements of criminal acts. This condition gives rise to differences in assessment at the judicial level, especially in cases involving anonymous digital identities, the use of third-party accounts, or crimes committed in an organized manner through electronic systems.

REFERENCES

- Adi Mansar, Rai Rake Setyawan Rai Rake Setyawan, Vania Micha Dwilizadi Vania Micha Dwilizadi, Duma Indah Sari Lubis, A. A. S. A. A. S. (2026). Reconstructing Restorative Justice Through Customary Criminal Law In Indonesia's Juvenile Justice System. *Jurnal IUS Kajian Hukum Dan Keadilan*, 14(2). <https://doi.org/https://doi.org/10.29303/ius.v14i2.2048>
- Arief, B. N. (2008). *Bunga Rampai Kebijakan Hukum Pidana Perkembangan Konsep KUHP Baru*. Kencana Prenadamedia Grub.
- Arief, B. N. (2018). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Kencana.
- Ayu Rahmania, M. Faisal Dio Azhary, F. F. A.-N. S. (2025). PENGARUH ALAT BUKTI ELEKTRONIK TERHADAP PEMBUKTIAN TINDAK PIDANA SIBER DALAM HUKUM ACARA PIDANA INDONESIA. *Causa: Jurnal Hukum Dan Kewarganegaraan*, 16(1). <https://doi.org/https://cibinstitute.id/index.php/causa/article/view/1162>
- Collins, J. (2026). The industrialisation of fraud: understanding fraud in a digital era. *Legal Studies*, 46(1). <https://doi.org/doi:10.1017/lst.2025.10101>
- Dennis Fernando, Dini Dewi Heniarti, C. A. F. Z. (2025). TRANSFORMASI ALAT BUKTI ELEKTRONIK MENGGUNAKAN DIGITAL FORENSIK DALAM PEMBAHARUAN HUKUM ACARA PIDANA. *Journal Justiciabelen (JJ)*, 5(1). <https://doi.org/https://doi.org/10.35194/jj.v5i01.5506>
- Dhimas Abie Thoyib, Adi Mansar, A. R. M. (2026). Analisis Pertanggungjawaban Pidana Korupsi Dana Investasi Pada PT Asuransi Angkatan Bersenjata Republik Indonesia (Studi Putusan Nomor: 49/Pid.Sus-TPK/2021/PN Jkt.Pst). *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, 4(3). <https://doi.org/https://doi.org/10.61104/alz.v4i3.5601>
- Erwin Asmadi, Adi Mansar, Triono Eddy, Mukti Fajar Nur Dewata, Farid Wajdi, N. B. G. (2024). Data theft and the law on protection of personal data: A thematic analysis. *Jurnal Hukum Novelty*, 15(2). <https://doi.org/10.26555/jhn.v15i2.27661>
- Erwin Asmadi, Adi Mansar, T. E. (2023). Actualization of criminal liability for personal data protection in the use of financial technology: a comparative study of Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 27 of 2022 concerning Protection of Persona. *DE LEGA LATA: Jurnal Ilmu Hukum*, 8(2). <https://doi.org/https://doi.org/10.30596/dll.v8i2.15252>
- Farah Farिकासari Firjatullah Faqih, M. M. (2026). Electronic Evidence in Proving the Mens Rea Element in Corruption Crimes: A Case Study of Abuse of Authority. *Veteran Law Review*, 9(1). <https://doi.org/https://doi.org/10.35586/velrev.v9i1.11175>
- Gusti Muhammad Andre, Barda Nawawi Arief, RB Sularto, Faiqah Nur Azizah, N. N. (2025). Proof of Element of Unlawfulness Acts in The National Criminal Code. *LAW REFORM*, 21(2). <https://doi.org/https://doi.org/10.14710/lr.v21i2.67253>

- Harahap, M. Y. (2016). *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*. Sinar Grafika.
- Nasution, S. I. (2025). Mens Rea: Fondasi Pertanggungjawaban Pidana Dalam Sistem Peradilan Pidana Di Indonesia. *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syari'ah*, 7(1). <https://doi.org/https://doi.org/10.24252/iqtishaduna.v7i1.61542>
- Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, 33. <https://doi.org/https://doi.org/10.1016/j.fsidi.2020.200908>
- Njoto, D. L. B. (2024). Rekonstruksi Asas Actus Non Facit Reum Nisi Mens Rea dalam Tindak Pidana. *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, 7(3). <https://doi.org/https://doi.org/10.54371/jiip.v7i3.3735>
- Siregar, P. A. S. (2019). Keabsahan Akad Jual Beli Melalui Internet Ditinjau dari Hukum Islam. *(EDUTECH) Jurnal Ilmu Pendidikan Dan Ilmu Sosial*, 5(1).
- Syukur, K. A. (2015). PEMBUKTIAN UNSUR NIAT DIKAITKAN DENGAN UNSUR MENS REA DALAM TINDAK PIDANA KORUPSI. *Jurnal Ilmiah Galuh Justisi*, 3(2). <https://doi.org/http://dx.doi.org/10.25157/jigj.v3i2.420>
- Tubagus Ahmad Ramadan, S. M. (2025). Deconstructing Intentionality: Legal Fallacies in The Indonesian Criminal Code's Approach to Mens Rea. *Asian Journal of Social and Humanities*, 3(9). <https://doi.org/https://doi.org/10.59888/ajosh.v3i9.564>
- Wahyu Sabrudin, Triono Eddy, A. M. (2024). OPTIMIZING THE KNOW YOUR CUSTOMER PRINCIPLE IN THE CASE OF MONEY LAUNDRY THROUGH THE ROLE OF BANKING FROM ISLAMIC LAW PERSPECTIVE. *Proceeding International Seminar of Islamic Studies*, 1.
- Wiarti, J. (2024). Legality of Electronic Evidence in Cyber Crime Cases. *Ahmad Dahlan Indonesian Law Journal*, 1(2). <https://doi.org/https://doi.org/10.12928/adil.v1i1.572>