New forms of fraud in the field of digital financial assets: psychological coercion, fake infrastructure, the role of messenger networks and the limits of the return of stolen funds

Author: Prof. Vasily K. Isaul

Date: 09.05.2026

Table of contents

To whom the article is addressed

The presented article is addressed not to the mass reader, but primarily to state structures, whose competence includes ensuring public, state and information security, preventing and combating crime, as well as analytical support of threats in the digital environment.

In its content, the material is criminological, law enforcement, preventive and partially counterintelligence in nature. He considers not individual episodes of digital fraud, but the messenger environment as an infrastructure of involvement in illegal practices, including fraud, illegal mediation, shadow financial schemes, recruitment mechanisms and the normalization of criminal demand.

First of all, the article is intended for law enforcement agencies, state and national security agencies, as well as regulators and government bodies in the digital sphere. We are talking about structures that counter organized crime, digital fraud, network threats, illegal information trafficking and other forms of illegal activity in platform and messenger ecosystems.

Secondly, the material may be of interest to security councils and interdepartmental coordination bodies, financial intelligence and financial monitoring bodies, the forensic and scientific community, legislators and developers of regulations, as well as to educational and preventive structures working in the field of youth policy, digital security and prevention of destructive involvement.

The orientation of the article to these categories of addressees is due to the fact that the focus is on instant messengers as an environment of criminal involvement, the infrastructural rather than episodic nature of threats, mechanisms of anonymization, routing, pseudo-reputation and psychological impact, as well as risks to public safety and law and order. At the same time, significant importance is attached to the need for a systematic state response, interdepartmental coordination, digital analytics and prevention.

If we determine the main target addressee, then the article is most intended for the leadership and analytical units of law enforcement agencies and state security agencies involved in countering organized crime, digital forensics, monitoring network threats, countering fraud and preventing the involvement of citizens in criminal digital ecosystems.

Summary

In recent years, fraud in the field of digital financial assets has acquired a qualitatively new character. If earlier crude and primitive methods of theft, designed for gullibility and technical illiteracy, prevailed, now more and more long-term, multi-stage, psychologically verified schemes are observed, in which the victim is not just deceived, but is consistently introduced into a state of false confidence, emotional dependence and loss of criticality. Of particular danger is the combination of three factors: pseudo-financial legend, social engineering and a fake digital environment that imitates legitimate exchange, exchange or investment activities.

The role of large messenger sites deserves special consideration, where an environment has arisen that combines anonymity, the rapid spread of advertising, network involvement, closed groups, poor traceability of chains of influence and the extreme speed of movement of potential victims between channels, intermediaries and ultimate perpetrators of the crime. Against this background, the spread of fraudulent schemes has become especially noticeable, hiding behind conversations about staking, arbitration, trust management, automatic earnings, collective trading and other forms of supposedly professional profit making.

This article considers new types of fraud, mechanisms of psychological processing, the device of fictitious stock exchanges, the role of the messenger environment, ways to get out of destructive involvement, as well as the practical limits of the return of funds, which in reality turns out to be extremely difficult and, in most cases, does not give the victim the expected result.

Introduction

The claim that digital asset fraud has increased no longer needs proof. However, simply acknowledging growth is not enough. Not only has the scale changed, but the very nature of the criminal impact. A modern fraudster looks less and less like an accidental Internet adventurer. On the contrary, he appears in the guise of a confident, outwardly prosperous, disciplined participant in the business environment. He can speak at public events, appear in business spaces, speak the language of financial analytics, demonstrate the office, assistants, reports, positive reviews and even the appearance of legal support. Before us is no longer a scattered deception, but a whole industry of imitation of legality.

It is especially disturbing that the victims of such schemes are not only people with low awareness, but also persons with education, professional experience, sustainable income and, at first glance, a sufficient level of rationality. The reason is that the criminal influence is directed not at ignorance as such, but at the vulnerabilities of the human psyche: the desire to control the future, the desire to restore lost opportunities, the fear of missing out on income, the thirst for recognition of one's own foresight, trust in status signals and a gradual shift in the boundaries of what is permissible.

Today, the criminal network is often arranged on the principle of division of labor. Some individuals form the flow of potential victims through advertising and pseudo-expert channels. Others engage in primary conversation, reveal the level of wealth, emotional profile, family circumstances, financial expectations and degree of suggestibility. Still others are connected as "analysts," "mentors," "managers," "exchange employees," "security service," "return lawyers," "unlocking curators." As a result, the victim is not in a conversation with one person, but inside a staged social environment, where each participant plays a role in the overall production.

That is why the conversation about new fraud schemes should be conducted not as a list of private tricks, but as a system of organized psychological and financial seizure.

Modern types of fraud: from gross deception to managed engagement

The most noticeable feature of recent years has been the shift from one-time theft to a long-term model of victim escort. The victim is no longer always trying to rob in the first minute. It can lead for weeks and even months, creating the illusion of growing trust, mutual benefit and a joint goal. This delay is necessary for the criminal for the main thing: not just to gain access to funds, but to make sure that the victim himself begins to protect the fraudster from doubts, rationalize what is happening and reject the warnings of loved ones.

Schemes are widespread in which a person is offered a safe entrance "from a small amount," then they demonstrate imaginary profits on a fake page, and then convince to increase investments. Criminals understand the fundamental law of victim behavior: a person is more willing to bring more money to where he allegedly saw the first success. At the same time, the first "results" can be completely drawn in your personal account, having nothing to do with the real movement of funds in the real market.

Another variety is a scheme with a false technical operation, when the victim is asked to perform an action on his account, in his wallet or in the application, without revealing its true meaning. They explain to him that these are "confirmation," "synchronization," "binding," "setting up protection," "moving liquidity," "opening a trade route," "connecting a strategy." In fact, it is at this moment that access is either transferred, or a malicious transaction is approved, or funds are sent to a non-returnable address, or the right to dispose of assets by a third party is connected.

Especially cynical schemes based on phased drawing into a false professional hierarchy. First, the "assistant" speaks to the victim. Then the "lead analyst" appears. After - "senior specialist in supporting large clients." Later, the "risk department," "security service" and "financial curator" are connected. Each new figure reinforces the suggestion that if so many people are involved, if they respond quickly and in concert, then the organization is real. This is how a criminal group turns its own mass character into an instrument of trust.

Finally, a separate line is formed by schemes in which theft is generally disguised not as deception, but as failure in a complex financial transaction. The victim is told that the funds are not stolen, but "frozen," "temporarily held," "transferred to a security reserve," "subject to verification of origin," "blocked due to risk," "require a counter payment" or "await unlocking after payment of the commission." So, the deception continues after the first theft: they are trying to extract even more funds from an already injured person, forcing him to "save" allegedly frozen assets.

Victim psychological processing: not mystical "reprogramming," but controlled destruction of critical thinking

We are talking about a consistent change in the regime of perception, risk assessment and decision-making under the influence of stress, expectation of reward, social dependence and information isolation. Scammers don't create new brains; they skilfully exploit pre-existing properties of the nervous system and behavior.

The impact in question is not based on a single deceptive message and not on a simple transmission of false information, but on a carefully organized sequence of affective states, which gradually subjugates the will of a person, shakes his

critical ability and transfers behavior from the field of rational decision to the field of controlled reaction. In everyday speech, such a mechanism is often conveyed by the simplified formula "dopamine - cortisol - dopamine," however, in the scientific and analytical presentation it should be emphasized that we should not talk about a literal laboratory measurement of neurochemical indicators for each specific victim, but about a holistic psychophysiological cycle reinforcement. Its essence is as follows: first, a person is presented with the image of a desired acquisition, evoking hope, inner uplift and expectation of imminent benefit; then an obstacle, risk, threat or time deficit is deliberately built into this picture, which creates anxiety, tension and fear of loss; after that, the subject is again offered the prospect of deliverance and reward, as a result of which hope flares up with renewed vigor. It is this alternation that forms a vicious circle in which the personality is less and less capable of an independent assessment of what is happening. Here the main thing is accomplished: a person ceases to think in the categories of truth and lies, probability and evidence, benefits and losses in their real content; he begins to think in the categories of emotional rescue, immediate relief, and a return to promised well-being.

It is fundamentally important that this impact is not reduced to the simple greed of the victim, as is sometimes superficially stated in low-level journalism. Before us is a much more serious and more alarming phenomenon: the purposeful use of the fundamental properties of the human psyche. Man is inherently inclined to respond to the promise of rare good fortune with internal mobilization; he is alert to the threat of loss; he seeks relief when the tension becomes excruciating. These reactions are normal. It is not the presence of such reactions that is pathological, but the fact that they are skilfully manipulated, building from them a consistent tool for suppressing critical judgment. Where the subject believes that he is making a free decision, in fact, the imposed logic of the emotional pendulum is already in effect.

At the initial stage, a person is offered not just a profitable offer, but a special image of his own exclusivity. This circumstance deserves the closest attention, since it is here that the foundation is laid for future dependence on the imposed scenario. The victim is convinced that he was not among the usual addressees of mass influence, but among the few who have a special opportunity, closed to the majority. He may be told about privileged access to information, early notification, admission to a limited operation, a trust channel for profit, a rare chance that only selected participants have. Outwardly, such messages can be framed in different ways, but their meaning is the same: a person must survive not just interest, but a sense of dedication. It is the sense of chosenness that becomes the first blow to critical vigilance.

The psychological significance of this technique is extremely great. Feeling privileged acts on consciousness as a powerful catalyst for trust. Where the usual situation would require caution, verification of the source, comparison of facts

and consultation with an independent specialist, another internal remark arises: not "I can be deceived," but "I am unusually lucky that I was among the first." This shift seems insignificant only at first glance. In fact, it is it that transfers a person from defense mode to engagement mode. It no longer guards its borders, but seeks not to miss what is presented as a rare opportunity. Moreover, the idea of one's own admission to closed knowledge often feeds pride. The victim begins to perceive participation in the scheme as confirmation of his own insight, foresight or special status. Here, not only selfish expectation is affected, but also more subtle strings - the need for recognition, the desire to feel outstanding, the desire to be not an object of external forces, but a dedicated participant in a significant process. And therein lies one of the darkest sides of the impact in question: it exploits against the individual not just his weakness but his legitimate pursuit of dignity.

At this stage, deceivers often avoid rough pressure. On the contrary, they act with emphasized restraint, as if providing the addressee with the opportunity to come to a favorable conclusion himself. Such imaginary unobtrusiveness has a deep calculation. When a decision is presented to a person by its own discovery, it takes root much more firmly than in the case of direct imposition. The victim begins to perceive subsequent actions as a continuation of his initiative, and not as submission to someone else's will. Thus, a subjective illusion of autonomy is formed, in which the degree of external control only increases. The illusion of self-selection becomes one of the key conditions for further subordination.

The next step is to introduce an alarm, but the alarm is strictly dosed. This is not chaotic intimidation or overt terror, but a finely calculated tension sufficient to narrow thinking but not yet so intense as to completely destroy interaction and trigger immediate withdrawal. It is the measure of alarming impact that is crucial here. If a person does not feel danger, he can postpone the decision, start checking, discuss the situation with other persons, turn to documents and thereby destroy the artificially created atmosphere of exclusivity. If the pressure turns out to be excessive, he can recoil, interrupt communication, suspect a criminal intent and get out of influence. Therefore, anxiety is introduced as if gradually, while maintaining the appearance of a rational explanation. It is reported about the time window of opportunity, about a sudden change in conditions, about the need to urgently confirm the action, about the risk of losing the already almost received benefit, about blocking funds, about additional verification, about the likely loss due to delay. At first glance, each of these messages may look plausible, especially if it is accompanied by business vocabulary, reference to rules, visibility of order and procedures.

Here it is necessary to emphasize that anxiety in such cases acts not only as an emotional shock, but also as a tool for changing the very structure of thinking. Under the influence of tension, the field of attention narrows. A person ceases to fully retain in consciousness all elements of the situation and begins to focus on

the closest irritant, which requires an immediate response. The ability to compare information in a long-time perspective decrease: it becomes important not how plausible the whole scheme is, but how soon to relieve the current concern. The tendency to independent verification is weakened, since all internal energy is directed to overcome acute discomfort. A kind of mental funnel arises: the stronger the anxiety, the narrower the horizon of reasoning; the narrower the horizon of reasoning, the higher the probability of impulsive action; the more impulsive the action, the deeper the involvement in the imposed scenario.

A key consequence of anxiety is the substitution of the purpose of behavior. Before the tension is turned on, a person could potentially seek to establish the truth: check the source, understand the legal and factual side of the case, establish whether there are real grounds for trust. After the alarm is turned on, its purpose changes. He is already striving not so much to learn the truth as to get rid of the painful uncertainty. This is a radical turning point. It is he who explains why victims often commit acts that would seem incredible to them in a calm state. They act not because they suddenly become less reasonable in the general sense of the word, but because their mind is forcibly transferred to the mode of urgent affective response. In other words, fraudulent exposure does not eliminate intelligence per se; it reconfigures it, forcing it to serve not the search for reality, but the search for immediate relief.

The fact that anxiety is almost always associated with the already promised benefit deserves special attention. A person is inspired not by an abstract danger, but by the danger of losing what he has already internally recognized as almost his own. Psychologically, this is extremely important. The loss of a hypothetical future is experienced much stronger when this future has already been emotionally appropriated. If the subject managed to imagine a profit, imagine its use, connect his plans and hopes with it, then the threat of the disappearance of this profit is perceived as taking away an almost really good. Hence the feverish willingness to pay, confirm, translate, agree, just not to lose the already mentally appropriated. So, the imaginary turns into the psychologically real, and then this real is used as a lever of pressure.

At the third stage, there is a promise of an early resolution of the crisis and a result. After artificially created tension, a person is offered not the final fulfillment of the promised, but the prospect of its inevitable achievement, subject to another action, another formality, another confirmation, another payment, another stage. It is here that one of the most stable mechanisms of dependent behavior is manifested - intermittent reinforcement. The reward comes and goes; either shown in symbolic form, then postponed under a new pretext; it seems almost received, then again obscured by an obstacle. This logic is the deep trap. The unpredictability of success often binds a person more firmly than a guaranteed and even result. The constant reward is satiating and soothing; variable reward excites, rivets and exhausts.

It should be especially emphasized that at this stage a person is often presented with signs of imaginary progress: notification of the completion of the procedure, messages about enrollment, indications of the readiness of funds for issuance, confirmation of the successful completion of the intermediate stage. All this plays the role not of a real result, but of its staging. The victim is not given the blessing itself, but is given his image, his shadow, his promise, his vestibule. So the painful state of "almost" is maintained. The affective power of this state is colossal. When it seems to a person that the desired is in one step, he transfers new requirements much more willingly than at the beginning of the journey. He argues not as it should be in conditions of sound caution, but as emotional inertia dictates: "after everything already invested, you cannot stop," "the last barrier remained," "if you stop now, the previous efforts will disappear." This includes not only the hope for profit, but also the unwillingness to admit the vain actions already committed. The more a person has invested - money, time, emotional energy, trust - the harder it is for him to break the chain internally. And therefore, each new promise of an "almost complete" result acts with increasing force.

In the mechanism under consideration, the rhythm of alternating hope and fear plays a special role. If the subject had only been promised, but not disturbed, he would have cooled down over time and began to doubt. If he had only been frightened, he would either have closed or broken the connection. But alternating these states produces a qualitatively different effect. Hope opens a person to exposure; fear makes him malleable; the new promise is not just comforting, but connects with the source of anxiety, since it is this source that now looks both the cause of suffering and the only guide to salvation. This is the paradoxical and terrible logic of manipulation: the one who creates the problem imposes himself as a means of solving it. This is how affective dependence on the mechanism of violence itself is formed. The victim begins to reach for the next message, for the next order, for the next promise of relief, although it is this sequence that keeps her captive.

From a scientific point of view, it is important to note that such cyclicality undermines not only individual decisions, but also the architectonics of subjective control itself. Repeated fluctuations between arousal and anxiety deplete the ability for sustained self-observation, disrupt the sequence of logical analysis, and increase suggestibility. A person ceases to rely on the general rules of reasonable diligence, because each new episode seems exceptional and urgent. The regular experience of emotional swings sets the stage for a kind of narrowing of the world: outside the framework of the imposed scenario, as if nothing remains. Close warnings, sound arguments, obvious contradictions, legal and factual inconsistencies - all this begins to fade before the dominant internal task: to finally complete what has begun and relieve the exhausting tension. This is how freedom of judgment is destroyed - not by a one-time order, but by a thousand emotional shocks, each of which individually may seem insignificant, but together forms a system of subordination.

It is also necessary to pay attention to the moral and social dimension of this phenomenon. Before us is not just a technique of illegal seizure of property, but a form of psychological encroachment on the human ability to reasonable self-determination. Here, the criminal calculation aims to turn hope into a hook, anxiety into a whip, and the promise of salvation into an excuse for new submission. This is a deeply inhuman practice, because it turns the basic mechanisms of a person's life orientation against himself. The fact that in normal social life helps the individual to strive for the best, recognize danger and look for a way out of difficulty, here turns into an instrument of exploitation. That is why such schemes should not be considered as a series of random tricks, but as systemic violence against the psyche, disguised as business communication, help, support or participation in a profitable operation.

As a result, the cycle described - the promise of reward, then alarming compression, then a new promise of deliverance and benefit - is one of the most effective models of victim involvement and retention. Its strength lies not in gross lies per se, but in the consistent management of a person's internal states. First, the subject is given hope, then peace is taken away, then hope is returned in exchange for obedience. And the longer this alternation continues, the weaker the independent judgment becomes and the stronger the emotional binding to the source of the impact. So, a dangerous form of submission is born, in which a person no longer freely assesses what is happening, but moves from one promise of relief to another, taking each new demand as supposedly the last step towards salvation. This is the central tragedy of such manipulative schemes: they do not just deceive a person, they rebuild the very course of his experiences in such a way that he begins to participate in his own deception, taking the imposed sequence as a path to liberation, while in reality it only leads to further dependence, loss of funds and destruction of personal autonomy.

The mechanisms of coercion and involvement described above are accompanied by personalized psychological profiling, which is not a random set of techniques, but a carefully built system of targeted influence on the internal stimulating forces of a person. Before us is no longer a gross deception in its primitive form, but a delicate work to extract from the personality those vulnerable contents that in ordinary life are hidden even from it. Criminals don't just collect information about age, income, marital status or professional experience. Their real task is different: to reveal what kind of internal deficit, what kind of hidden tension, what kind of unreflexed anxiety make a particular person susceptible to the promise of imaginary salvation. That is why, in the course of communication, they listen extremely carefully to intonations, note repeated formulations, notice emotional reactions to topics of wealth, status, parental duty, social recognition, lost opportunities, aging, social failure and personal guilt.

Here it is necessary to emphasize: fraudulent influence becomes especially effective when it ceases to be impersonal and begins to imitate a deep

understanding of personality. If a person, for example, lives in a stable fear of poverty, he will be offered a story not about reckless risk, but about reliable preservation of funds, protection of accumulated, reasonable foresight and a responsible attitude towards the future. If a person with a pronounced ambition, painfully experiencing his own underperformance, is presented with a completely different picture: not frugality, but a breakthrough; not conservation, but growth; not protection, but a welcome proof of one's own strength and exceptionalism. Anyone who is tormented by guilt in front of his family will hear the legend about the possibility of finally "doing the right thing," "providing for loved ones," "correcting past mistakes," "giving children what he himself was deprived of." A person striving for independence and internally tired of dependence on someone else's assessment will be inspired by the idea of a mature, sovereign decision, the right not to explain anything else to anyone, about financial action as a symbol of adulthood and personal subjectivity.

Of particular note is the fact that each legend is not built around the financial action itself, but around a psychologically significant meaning for the victim. In other words, a person is sold not a transfer of funds, not an investment, not participation in a scheme, but an emotionally charged image of himself. One begins to see himself as a cautious and wise custodian of capital. Another is a man of rare insight, able to recognize a unique price difference and take advantage of it earlier than others. The third is a disciplined builder of long-term affluence. The fourth is an elected member of a closed circle, access to which is allegedly obtained only by the most informed and worthy. In each case, we have the same criminal plan, but it is clothed in different ideological forms, depending on which personality image is most desirable for a particular addressee. This circumstance is extremely important for scientific analysis, since it allows you to see: deception does not act contrary to a person's pride, but through him; not through crude suppression of will, but through flattering attachment to her hidden aspirations.

Therefore, personalized profiling needs to be seen as a form of applied psychological abuse in which the perpetrator temporarily assumes the role of interpreter of the victim's inner life. He seems to tell a person: "I understand you better than others, I see your true needs, I know the way to their satisfaction." It is this usurpation of the role of the understanding interlocutor that creates the primary dependence. A person, especially one who is in a state of protracted anxiety, uncertainty or life fracture, tends to reach for someone who offers not only a remedy, but also an explanation. And the more convincing this explanation is embedded in an existing personal drama, the stronger the trust becomes. As a result, the criminal scheme begins to be experienced not as external pressure, but as a long-awaited response to an internal request. This is one of the most dangerous aspects of modern fraudulent practices: they parasitize not only on ignorance, but also on the most intimate motives of human existence.

No less essential element of the criminal impact is the destruction of external sources of correction, that is, the consistent weakening or discrediting of those social ties and institutions that could return the victim to a critical perception of what is happening. It should be said with all certainty: the isolation of the victim is not a side effect, but a central tool for keeping it inside the inspired picture of the world. As long as a person retains a lively connection with loved ones, professional consultants, banking specialists, lawyers, law enforcement officers or simply sane acquaintances, the criminal structure remains vulnerable. Any external voice is able to ask a simple but destructive question for the scheme: where are the legal guarantees, what is the real mechanism for generating income, to whom exactly the funds are transferred, why is it necessary to rush, why is it forbidden to discuss this with relatives, why are promises not supported by documents? That is why scammers seek to intercept not only the attention of a person, but also the very system of criteria by which he distinguishes reality from inspired fiction.

This process often begins gently, almost imperceptibly, under the guise of friendly care or expert caution. The victim is told that relatives "think in the old way," "are afraid of everything new," "never understood great opportunities." Banking institutions are exposed by structures that allegedly jealously protect their own monopoly on cash flow and therefore impede any form of "free" capital growth. State bodies are portrayed as clumsy, formal, divorced from modern economic reality, unable to understand new forms of property relations. Any critical individuals are declared either incompetent, dependent, or internally envious beforehand. Here we have a truly classic picture of destructive influence: all external sources of verification are declared suspicious, and a group of manipulators becomes the only bearer of truth.

Of particular danger is that such isolation is almost never served as isolation. On the contrary, it disguises itself as enlightenment, dedication and protection from "someone else's misunderstanding." The victim is told that her entourage is unable to appreciate what is happening due to their own limitations, conservatism or intellectual unpreparedness. Thus, a person receives not just a ban on appealing to external opinions, but a seductive explanation why such appeals seem to be meaningless and even harmful. A vicious circle arises: the stronger the external voices object, the more convincing, according to the victim, is the thesis about the hostility or incompetence of these voices. This is how criminals achieve an amazing result: the very fact of a warning begins to work not against fraud, but in its favor, since it is interpreted by the victim as confirmation of a previously inspired scheme.

From a scientific point of view, this mechanism can be characterized as an artificial narrowing of the epistemic environment of the individual, that is, a deliberate reduction in the number of recognized sources of knowledge and assessment. A person ceases to correlate the statements received with

independent criteria and increasingly checks them only with the opinion of those who are already interested in preserving the delusion. In such an environment, even obvious contradictions lose their destructive power, since there is no instance that can give them proper meaning. The delay in payments is explained by the "technical procedure," the requirements for additional transfers - "the need to complete the cycle," the refusal to submit documents - "confidentiality regime," requests not to disclose details - "protection from ill-wishers." What outside the isolated circuit would look like an obvious sign of a criminal scheme, inside it begins to be perceived as a normal part of the "complex process," understandable only to initiates. This is how a dangerous intellectual dependence is born, in which a person is no longer able to independently restore the criteria for reliability.

Finally, shame occupies a key place in victim retention as a tool for post-criminal linking of a person to a perfect mistake. It is this phenomenon that explains why, even after the first serious suspicions appear, a person often does not stop participating in the scheme, but, on the contrary, continues to invest in it morally, emotionally and financially. It should be emphasized: criminals are well aware that the exposure of deception does not take place in an empty psychological space. It faces powerful internal resistance, since admitting to being deceived means not only stating the loss of funds, but also surviving a blow to one's own self-esteem, intellectual identity, social image and idea of one's own maturity. For many people, this experience turns out to be more painful than the most property damage.

Shame is especially dramatic for those with a high level of education, a steady income, a pronounced sense of competence and a habit of considering themselves rational. The stronger a person is connected with the image of a "reasonable," "prudent," "unvarnished" subject, the more painful it is for him to face the fact of his own vulnerability. A severe internal gap arises: reality is already giving signals of danger, but recognition of this danger requires a revision of self-perception. And it is in this crack that criminals build the next level of control. They strive to induce the victim as early as possible to take actions that will not only be financially significant, but also morally compromising from her own point of view: transfer money against the advice of loved ones, borrow funds from relatives or acquaintances, hide the operation, lie about its content, violate previously declared rules of caution, neglect your own principles of discretion. After that, a person is no longer bound by one hope for profit, but also by the painful need to avoid humiliating recognition.

As a result, an extremely dangerous psychological node is formed, in which shame begins to perform the function of an internal censor and an internal overseer at the same time. The victim is afraid not only to lose funds, but also to meet with questions from others, with their bewilderment, with possible sympathy, which is sometimes even harder than condemnation. He postpones

the appeal for help, silent facts, minimizes the scale of involvement, convinces himself that the situation is still reversible. Moreover, he can make new translations not because he sincerely believes the promises, but because each next concession delays the moment of final recognition of the disaster. One of the most tragic paradoxes of fraudulent influence is revealed here: the continuation of participation in the scheme is experienced as less painful than the recognition of a deception that has already happened. In other words, illusion becomes anesthesia, and hope becomes the last defense against a crushing blow.

It must be strongly emphasized that this shame is not a private emotional reaction of an individual victim; it represents a socially and culturally mediated mechanism that criminals knowingly exploit. In many societies, financial imprudence is perceived not simply as a mistake, but as a sign of weakness, naivety, lack of intelligence or character. That is why the victim is often afraid not only of real condemnation, but also of an imaginary sentence, which, as it seems to him, will be passed by his entourage. He hears these future remarks in advance, sees disappointment in the eyes of loved ones in advance, experiences humiliation in advance. This foreshadowed shame is enough to keep quiet when an urgent appeal for help is required. In such a situation, silence becomes not passivity, but a form of desperate self-defense, although it is this that works in the hands of criminals.

Thus, we can conclude that the mechanisms considered form a single system of phased subordination of the individual. First, criminals recognize the leading motive of a person and create an individual legend for him, in which financial action appears as a solution to a deep life problem. Then they destroy or discredit external sources of correction, depriving the victim of the opportunity to check the inspired picture with independent reality. After that, shame is introduced into the course as a means of finally consolidating involvement: a person no longer just hopes for the promised result, but is also afraid to admit that his trust was used against himself. Together, these techniques do not form a chaotic chain of tricks, but a slender architecture of psychological submission, in which each next stage builds on the previous one and strengthens it.

That is why the fight against such crimes requires the rejection of a simplified, accusatory view of the victim. The victim of fraud is not a "greedy simpleton," but a person who has been subjected to multi-level effects on his fears, hopes, social ties and moral self-awareness. As long as public discourse is built on ridicule, contempt or moralizing, criminals will continue to enjoy one of their strongest allies - the shame of silence. On the contrary, an adequate scientific and social approach must proceed from the fact that vulnerability to skillfully organized deception is not an exception, but part of human nature. Recognition of this fact does not weaken the requirement of personal caution, but returns the necessary sobriety to the discussion. And if we really strive to resist modern forms of fraud, then we must see in them not only an encroachment on property, but also a

systematic invasion of the mental autonomy of the individual, aimed at subordinating the will, destroying critical judgment and exploiting the most painful internal experiences of a person.

False infrastructure: fake exchange sites, fake personal accounts and imitation of the trading environment

One of the most dangerous and at the same time the least properly meaningful phenomena in the structure of modern property deception is a fake digital infrastructure that skillfully reproduces the external signs of an exchange, exchange node, intermediary trading organization, investment account or personal account of a participant in operations. It should be emphasized: in this case, we are not talking about a single false site, not about a roughly executed fake, and not about a random set of misleading pages. A whole-built deceptive environment often unfolds in front of the victim, in which each component - from the color scheme and the location of the sections to the pseudo-documentary accompaniment and the sequence of messages - is subordinated to one task: to deprive a person of the ability to critically assess what is happening and replace fact-checking with a psychologically convenient illusion of reliability.

The essence of such an infrastructure is that it reproduces not so much individual signs of legitimate financial activity as the very feeling of institutional reliability. A person sees in front of him not a chaotic fraudulent page, but an ordered space resembling the usual environment of modern cash turnover. That is why the danger here is determined not only by the degree of technical equipment of criminals, but above all by the depth of their understanding of human perception. They don't just draw tables and charts; they construct trust as a manageable psychological process. The victim gradually gets used to the interface, begins to perceive it as a working tool, ceases to doubt the reality of the information displayed and, which is especially significant, internally transfers to the criminal structure the credit of trust that in ordinary life is associated with banks, exchanges, state control, legal procedures and business documentation.

The first fundamental sign of such an environment is pseudo-realism, that is, the deliberate creation of a convincing, outwardly plausible picture of financial activity that has no real economic content. The corresponding resource may contain charts of price movements, tables with quotes, history of actions taken, sections of identity confirmation, windows of alleged operational support, pop-up notifications of accrued profits, reports on imaginary operations, links to service rules, permits, user agreements, information on long-term work experience of the organization, and sometimes sections with fictitious analytical reviews. However, the abundance of these elements not only does not confirm the reality of economic activity, but often directly serves to conceal it. Before us arises the paradox of modern criminal disguise: the richer the visual and text

shell, the more difficult it is for an unprepared person to notice the absence of a genuine subject that she must certify.

It is fundamentally important to note that external plausibility is not identical to legal and economic reality. The chart alone does not prove the existence of bidding. The table does not certify the fact of the circulation of assets. An indication of a permit does not confirm its validity if it is not verifiable through official state registers. The history of operations does not indicate that at least one of them actually happened. Even the presence of carefully drawn up internal provisions, formally sustained in a business style, often serves not as a sign of legitimacy, but as an instrument of suggestion. This is precisely one of the most dangerous aspects of the phenomenon under consideration: decoration begins to replace evidence, and form - to replace content.

Pseudo-realism is particularly powerful because it relies on a belief deeply ingrained in the mass consciousness: if something looks complicated, orderly and professional, then it is probably authentic. The fraudulent environment exploits this belief mercilessly and systematically. It creates the impression of technical richness, legal design and organizational maturity. The victim is not affected by one specific element, but by a set of agreed signals, each of which individually may seem unconvincing, but together they produce a powerful effect of institutional credibility. A person sees familiar designations, familiar categories, seeming business discipline, repeatability of operations, internal interface logic - and it is this combination that makes him perceive lies as probable truth.

It should be said with all certainty: in such cases, the victim is shown not the market, but the stage reproduction of the market, not the actual turnover of values, but a carefully set idea of such a turnover. This is not a space of genuine exchange, but a space of controlled impression. Its architecture is designed to remove the natural question from a person: "Where and how is the operation actually performed?" Instead of an answer, he is offered a spectacle sufficient for emotional reassurance, but empty in terms of verifiable reality. Here the crime is committed not only by direct withdrawal of funds, but also by organized visibility, which temporarily replaces the victim with facts.

The second key feature is visual profit when it is actually impossible to dispose of funds, primarily the impossibility of returning or withdrawing them. On the screen, the victim's account balance can grow, income can be displayed, interest can be charged, the indicator of total profitability can increase, supposedly successful operations can be recorded, imaginary profitable positions can be closed. Sometimes a person is even shown the dynamics of his "investment path": entry fee, intermediate growth, acceleration of profits, achievement of a new status, admission to "expanded opportunities." Outwardly, all this creates the impression of capital movement and successful participation in profitable activities. But this profit exists only within the criminal interface and exactly until the victim remains a source of new income.

It is the attempt to get the money back that becomes the moment of truth in which the deceptive construct reveals its genuine purpose. As soon as a person expresses his intention to withdraw funds, new obstacles immediately arise, filed under the guise of mandatory procedures: payment of tax, commission coverage, confirmation of the origin of funds, payment of an insurance premium, provision of a withdrawal channel, activation payment, status confirmation, temporary regulatory fee, liquidity reservation, account security check, synchronization restoration, repayment of internal debt, confirmation of the transit limit. The names may change, but the logic remains unchanged: the right to receive their own money is made dependent on a new transfer in favor of criminals.

Special attention should be paid to the fact that such a scheme has exceptional psychological effectiveness. If the victim were immediately informed that the money was lost, further extortion would become difficult. But criminals act thinner. They seek to convince a person that the funds have not been stolen, have not disappeared, have not been withdrawn by third parties, but are still registered with him, albeit temporarily unavailable due to some formal procedure. This is an extremely important point. A fake personal account is needed not to store money, but to store hope. While the amount is saved on the screen, while the income is growing, while the system promises an early completion of the check, the victim is inclined to perceive the next payment not as a new loss, but as a condition for the future return of already "available" funds.

This is how one of the most destructive mechanisms of modern digital extortion arises: a person is not just once deprived of money, he is drawn into a chain of consecutive payments, each of which is justified by the previous one. The amount already paid psychologically pushes him to pay again so as not to "lose everything completely." In the scientific literature, such a process is described as an increase in forced involvement, but in the journalistic dimension it is necessary to call a spade a spade: we have a cruel exploitation of human hope, fear and shame. The victim is afraid to admit that he was deceived; it is easier for him to believe in another formality than in the scale of the damage suffered. Criminals know this excellently and build their false infrastructure in such a way that each next payment does not seem absurd, but the last necessary step to unblocking the account.

Therefore, the displayed profit does not perform an economic, but a purely manipulative function. It is needed to maintain trust, to suppress doubts, to justify new requirements, to extend the time of contact with the victim. In other words, profit in a fraudulent office is not the result of activity, but a means of further pressure. The more convincing the growing balance looks, the more difficult it is for a person to admit that he is just a numerical illusion, not provided with either an asset, an obligation, or a real possibility of disposal.

The third system-forming sign is the substitution of concepts between a genuine exchange and a criminal superstructure, artificially presented as part of a

recognized, large and supposedly legitimate financial system. Criminals can use names, color combinations, styles, conventions, site addresses similar to those of well-known sites. Sometimes they directly copy the composition of pages, the style of service sections, the structure of the menu, the nature of notifications. In other cases, they go even further and claim that they are acting not on their own behalf, but as a "partner office," "closed gateway," "internal circuit for large customers," "service interface," "special billing section," "auxiliary platform for verified participants." For an unprepared person, such terminology sounds weighty, difficult and therefore convincing. But it is in this complexity that the trick lies.

The substitution of concepts acts due to the fact that criminals rely on the asymmetry of knowledge between themselves and the victim. An ordinary person, as a rule, is not obliged to understand the structure of the exchange infrastructure, in the order of admission to trading, in the legal status of intermediaries, in licensing forms, in the delimitation of functions between the organizer of trading, the depository institution, the settlement organization and the market participant. Attackers use this incomplete knowledge without a trace. They fill communication with words that give the impression of professional depth, but do not contain verifiable meaning. The victim is inspired by the idea that before her is not an independent dubious resource, but only a special entrance to the already known large system, accessible to a limited circle of people. So, the criminal structure hides in the shadow of someone else's authority, parasitizing on the reputation of real organizations.

Of particular danger is the fact that such a substitution of concepts is often not reduced to a simple similarity of names. It includes the creation of a whole legend: a person is explained that the usual site of the exchange is intended for general acquaintance, and the investor's office is supposedly located in a different contour; those large transactions are not displayed in the public part; that there is a special connection order for "professional participants"; that withdrawal services go through a separate service section; that security requires the use of a "closed channel." This legend is designed for one thing - to normalize the anomaly, that is, to force the victim to consider suspicious signs not as evidence of deception, but as a consequence of his own ignorance.

As a result, a person ceases to compare what he saw with objective reality and begins to correlate it with the internal logic imposed by criminals. If the site address does not match the official one, this is due to "service access." If there is no open information in the registers, this is declared a consequence of the "international mode of operation." If the withdrawal of funds is delayed, they refer to "features of a large turnover" or "verification of interstate transit." If new payments appear, they are called "settlement support conditions." So, step by step, the fraudulent add-on pretends to be a technical continuation of the legal

system, while in reality it exists solely to intercept funds and keep the victim in a state of dependent expectation.

More broadly, the phenomenon in question signals a profound transformation of the very mechanism of fraud into the digital age. If earlier deception was often based on one false promise or on a brief episode of misleading, today we are witnessing infrastructure fraud, that is, a crime masquerading as a stable, multi-level, procedurally rich system. This is no longer a random trick, but a quasi-institutional construction, striving to reproduce the signs of order, regulations, accounting, reporting and official communication. It invades an area of public trust where a person is used to relying on formalized signs of legality. And that is why the damage from it goes beyond private property losses. The very trust in digital forms of economic organization, in remote methods of participation in financial turnover, in the language of business documentation, in external symbols of legitimacy is at risk.

This implies a fundamental conclusion: when assessing a suspicious digital environment, it is necessary to proceed not from the beauty of the design, not from the complexity of the interface and not from the saturation of pseudo-legal elements, but from the question of the verified connection between the displayed information and real legally significant activity. Is there a genuine legal entity? Is his status confirmed by official sources? Is there a valid right to provide the relevant services? Is it possible to check addresses, details, permits, dispute resolution procedure, a real mechanism for storing and transferring funds? Is the actual, not declared, ability to dispose of money provided? If there is no clear and independently confirmed answer to these questions, then we are most likely not a financial institution, but a skilfully made trap, the purpose of which is not to provide access to the market, but to seize the victim's funds under the guise of access to the market.

Thus, fake digital infrastructure should be considered as one of the central tools of modern fraud precisely because it combines visual plausibility, the numerical illusion of profit and conceptual mimicry for recognized institutions. Within its limits, lies cease to be a separate statement and turn into a holistic habitat for the victim. And this is her special public danger. A person is deceived not only by words, he is deceived by space, order, procedure, visibility of accounting, rhythm of messages, pseudo-documents, imaginary official necessity. He is convinced that he is inside the system, while in fact he has long been inside the criminal plan. That is why the scientific and law enforcement understanding of this phenomenon requires extreme accuracy, rigor and intransigence: where imitation of financial reality begins to replace reality itself, not just deception arises, but a highly organized form of encroachment on property, trust and the rational ability of a person to resist lies.

It is especially significant that in modern criminal practice, the greatest effectiveness is demonstrated not by primitive schemes of direct luring of funds,

but by complex, carefully staged structures based on psychological pressure, imitation of the professional environment and the creation of a sense of rationality in the victim. One of the central tools of such an impact is a false digital infrastructure, which not only accompanies deception, but forms its content core. It is she who turns the unfounded promise of income into an allegedly observable reality, replacing the genuine check with a skilfully built system of visual, numerical and procedural confirmations. We are not talking about random fakes of low quality, but about holistic technical decorations that reproduce the appearance of trading floors, accounting offices, notification services, analytical sections and calculation windows. Their purpose is to deprive a person of the main protective ability - a doubt based on independent fact-checking.

Especially often criminals exploit plots that have already become widespread in the mass consciousness and therefore are perceived as believable. First of all, we are talking about inter-exchange arbitration, that is, about the supposedly existing ability to extract almost risk-free profits due to differences in prices for the same asset at different sites. For an inexperienced participant, such a scheme sounds convincing: they explain to him that the market allegedly does not have time to equalize quotes, and therefore a fast performer of operations can receive stable income almost automatically. However, this is where fake infrastructure proves indispensable. Without it, the attacker would have to confine himself to words; with her, he gets the opportunity to show the victim a carefully constructed picture of the world, in which price gaps seem to exist constantly, transactions seem to be executed instantly, and profit seems to be fixed with mathematical inevitability. The screen displays tables with courses that differ in the desired direction, graphs designed to inspire a sense of market authenticity, windows for executing orders, transaction logs and total income amounts. But all this data exists only within a closed system of deception: they are not confirmed by any external and independently verifiable site, not a single publicly available source of exchange information, not a single legally significant document.

Equally often used is the scenario of repeating deals after the so-called successful participant. It is presented as a form of simplified entry into the sphere of circulation of digital assets: the victim is offered not to make decisions on his own, but only to follow the actions of an experienced person, whose high profitability has allegedly already been proven. From a psychological point of view, this is an extremely strong technique, since it removes the burden of one's own analysis from a person and transfers trust to the figure of a "mentor," "analyst" or "group leader." In this case, the fake infrastructure performs a double task. On the one hand, it creates an image of existing professional activity: it demonstrates supposedly opened and closed positions, time stamps, interest rates, history of previous operations. On the other hand, it forms the victim's sense of inclusion in a privileged community, where knowledge allegedly comes from a more experienced person to a less experienced one. This is how the most

dangerous illusion of indirect competence arises: a person convinces himself that he personally may not understand the subject, since he has already joined the one who understands. Meanwhile, all "signals," "inputs," "outputs" and "confirmations of the result" can be completely staged. It is easy to create a transaction log retroactively, the profitability is drawn arbitrarily, the sequence of actions is adjusted to the desired narrative effect. The more convincing this pseudo-documentation is, the less likely the victim will demand to compare what he saw with independent information about the movement of funds on a valid network or with the data of a legitimate trading platform.

Equally characteristic is the plot of highly profitable programs for blocking funds for the sake of reward, where criminals use the idea that simply holding an asset in a certain mode in itself can bring significant and, most importantly, regular income. And here the false digital environment becomes not an addition, but the main mechanism of suggestion. The victim is shown the amount of the allegedly placed amount, daily or hourly accruals, the growing total of income, the prospect of increasing remuneration when extending participation or making additional funds. In some cases, even technical restrictions on output are imitated to explain why a person sees profit on the screen, but cannot dispose of it immediately. He is informed about the need to pay an additional "confirmation fee," "tax," "insurance reserve," "unblocking fee," after which they promise to open access to the entire amount of funds at once. Before us is one of the most destructive forms of digital deception: the appearance of accrual replaces real property law. While the victim observes the growing numbers in the accounting window, he is inclined to consider them as property already belonging to him, although in reality there is no income to be received. False infrastructure makes a substitution: instead of a genuine civil-legal and technological result, a person is offered a theatrical spectacle of numbers.

The essence of the danger lies in the fact that such systems do not just demonstrate non-existent price discrepancies, non-existent profitability and non-existent accruals. They create an artificial confirmation environment in which each subsequent false message relies on the previous one and is therefore perceived as part of an internally consistent picture. The victim sees that the words of the "mentor" are allegedly confirmed by the movement of quotations, the execution of orders, an increase in income and messages about the status of the account. This consistency is deceptive, but it is she who has the strongest effect on consciousness. A person stops looking for external criteria for truth, because inside the fraudulent structure, all elements already mutually "prove" each other. As a result, the culture of verification itself is destroyed: instead of referring to independent registries, legal information about a person, real network data, the organization's reputation, the terms of the contract and the procedure for disposing of funds, the victim remains inside the fake digital space, taking its internal consistency as a sign of authenticity.

Criminals often resort to fake notifications from the security services, which deserves special attention, since here the false infrastructure turns from a tool of suggestion into a direct theft mechanism. The victim receives a message issued as an urgent warning about suspicious activity, the threat of hacking, the need to "save" the account, undergo additional identity confirmation, or immediately transfer assets to a "safe storage environment." Such notifications can come through e-mail, imaginary service windows on a fake site, messages in instant messengers, phone calls, or even through pseudo-official accounts on public networks. Outwardly, they are often designed with a high degree of plausibility: the names of well-known sites, the style of business correspondence, templates of alarm notifications, links to internal rules, threats of temporary blocking of the account when inactive are used. The main goal of such an attack is to force a person to perform an action in a state of controlled anxiety, when the fear of loss of funds suppresses the ability to reason.

This action can take various forms, but in all cases it is aimed at losing control over property or the means of disposing of them. The victim may be persuaded to transfer assets to an address issued as "reserve" or "protective," although in reality it belongs to criminals. He can be persuaded to approve a malicious permission to dispose of assets, allowing an unauthorized person to subsequently write off funds without separate approval of each transaction. He may be forced to disclose classified data - source keywords, private keys, one-time confirmation codes, account login information. Finally, it can be brought to the connection of remote access to the device, after which the criminal gets the opportunity to observe the actions of the victim, intervene in them, replace details, initiate operations or extract confidential information directly. This manifests a particularly sinister function of false infrastructure: it no longer only depicts the existence of income or threat, but also organizes a specific sequence of actions during which property is removed from the authority of the rightful owner. In other words, we have before us not just decorative support for fraud, but its full-fledged operational channel.

It should be emphasized that the high visual level of a digital resource does not in itself prove absolutely nothing. This circumstance requires fundamental and repeated repetition, since a significant part of users is still guided by external persuasiveness. A beautiful interface is not proof of legal, technical or financial reality. In the era of ready-made templates, public design libraries, inexpensive development tools and mass distribution of other people's samples, a criminal group is able to create such a digital facade in a short time, which, according to its external impression, will look even more impressive than the resources of many legitimate organizations. Moreover, it is illegal projects that often invest special efforts in visual decoration, because they need to compensate for the lack of real content. Where there is no proper legal status, an understandable organizational structure, a transparent procedure for accounting for funds, a provable history of activity and true responsibility to the client, there is a need for hypertrophied

visual persuasiveness. So fraudulent aesthetics becomes a surrogate for institutional reality.

Hence the key methodological conclusion follows: the main question is not in the beauty of the interface, but in the verifiability of the legal, technical and financial reality of the site. Legal verifiability presupposes the presence of a certain person responsible for the activities of the resource, the availability of information about its legal status, jurisdiction, dispute resolution procedure, terms of the contract, rules for the provision of services, and the mechanism for protecting user rights. If the person collecting funds is hidden behind anonymous designations, does not disclose his actual name, does not provide intelligible documentation or operates with vague formulas instead of legally significant obligations, this should already be considered as the hardest alarming sign. Technical verifiability means the ability to independently verify that the displayed operations are actually performed, that addresses and movements of funds exist outside the site interface, that the software permissions requested by the system meet the stated goals and do not go beyond the required. Financial verifiability, in turn, requires an answer to the simplest, but most inconvenient questions for fraudsters: where does the income come from, due to what economic mechanism it is formed, who takes the risk, what confirms the payment obligations, whether there is a documented and actually secured source of funds. Where instead of such answers only beautiful diagrams, admiring reviews, urgent appeals not to miss the opportunity and references to the success of a certain "mentor," one should see not an investment opportunity, but a high probability of criminal encroachment.

The particular public danger of the schemes under consideration is aggravated by the fact that they blur the traditional ideas about the signs of fraud. For a significant proportion of citizens, crime is still associated with gross forgery, the obvious absurdity of promises or the primitive speech of an attacker. However, the modern criminal environment has long overcome this stage. Today, deception is often served by the language of rationality, discipline, and technical competence. The victim is offered not to take their word for it, but to "see for themselves" - but he is forced to be convinced inside a pre-adjusted system. He is offered not to take risks, but to "follow a proven strategy"; not to rush, but to "act according to the regulations"; do not trust random people, but work with a "curator" or "security service." This is a deep paradox: the fraudulent scheme borrows the vocabulary of caution, verification and professionalism in order to destroy real caution, real verification and real professionalism with even greater efficiency.

Therefore, in scientific and practical terms, it is extremely important to consider false digital infrastructure not as a secondary shell of a crime, but as an independent subject of analysis. It combines the properties of psychological weapons, a technical intermediary and an organizational theft mechanism. Trust is created through it, dependence on the "mentor" is formed through it, profits are

staged through it, false alarms are distributed through it, and the final withdrawal of funds or means of access to them is made through it. While this infrastructure remains opaque for the user, he is in the position of a person who is offered to judge the reality of the institution solely by the majestic facade, not allowing him to look into the constituent documents, books, or the technical journal of operations. The whole power of the criminal structure rests on replacing the provable - plausible, the verifiable - spectacular, and the real - conveniently shown.

That is why the fragment under study requires the most categorical conclusion. No digital platform should be evaluated on the degree of visual persuasiveness, the number of animation elements, the smoothness of communication "support" or demonstrated profitability. The only significant criterion remains the ability of external, independent and reproducible confirmation of all significant circumstances: the existence of the organization, the legality of its activities, the validity of operations, the authenticity of obligations and the reality of the mechanism for generating income. When, instead of such confirmation, the user is offered only an internal picture without access to an independent audit, he is not dealing with a financial or technological system, but with a carefully staged presentation, where each detail serves one purpose - to deprive him of property under the guise of a reasonable and controlled action. This is the essential danger of false infrastructure: it does not just deceive the eye; it destroys the very ability to distinguish between the proven and the shown.

Messenger networks as an environment of accelerated involvement: the special role of Telegram

Telegram deserves special attention in a modern study of digital fraud as a special communication environment in which anonymity, the swiftness of the dissemination of information, the multiplicity of exposure channels, the ease of forming closed communities and the relative ease of transferring a potential victim from a visible public space to isolated personal communication are combined with exceptional density. It is this combination of properties that gives this site a fundamentally different public weight. Before us is no longer just a means of transmitting messages and not just a technical intermediary between users, but an established environment of systemic influence, within which the search for vulnerable persons, trust construction, imitation of competence, reputation signal management, psychological support of the victim and subsequent redirection of funds are carried out. In other words, Telegram in this kind of schemes acts not as an external background, but as a functionally rich social infrastructure, where each technical tool can be turned into an instrument of persuasion, concealment and submission.

At the same time, scientific conscientiousness requires a decisive rejection of primitive judgments. It would be methodologically erroneous to declare the site itself an identical criminal activity. Such a statement of the question does not

stand up to criticism already because any digital environment, possessing a neutral technical basis, is used by many subjects for legitimate, socially useful and socially significant purposes. However, the opposite extreme would be no less erroneous - the desire not to notice the obvious: it was in Telegram in recent years that an extremely favorable environment for fraudulent networks has developed, since the totality of its organizational and communicative properties makes it possible to build deception not sporadically, but as a stable, multi-link and reproducible process. Scientific analysis should be freed from both moralizing simplification and technical naive neutrality. The question is not whether the site as such is "to blame," but which properties of the environment objectively lower the threshold for abuse, accelerate the spread of deceptive practices and make it difficult to externally verify statements.

First of all, it should be noted that Telegram creates unique conditions for combining mass coverage with the illusion of personal intimacy. In a traditional public message, the addressee is clearly aware that he is dealing with addressing many persons at the same time. In the environment under consideration, this boundary is blurred. The channel can speak with thousands of subscribers, but stylistically and psychologically refer to everyone as a long-known interlocutor. This form of communication produces a powerful effect of engagement: the message is not perceived as impersonal advertising, it is experienced as trust advice, as a warning "for its own," as an exclusive invitation to the circle of initiates. This is where the psychological disguise of a commercial or criminal interest arises as an author's statement, which is extremely important for fraudulent schemes. The deception ceases to look like a crude imposition of a service; it begins to seem part of the natural information flow, part of the author's supposedly sincere personal position.

That is why Telegram channels are so convenient for quick acquisition of advertising placement and so dangerous due to their ability to hide the advertising nature of the message. Externally, a publication can be framed as a private opinion, personal experience, analytical observation, friendly recommendation, or even as a moral position of an author who wants to "warn" the audience and at the same time offer it a "reliable way out." But behind this rhetorical shell, paid material is often hidden, the purpose of which is not to inform, but to translate the attention of the subscriber to a pre-prepared link of the scheme. Disguising the goal as a form of sincerity becomes one of the central mechanisms for legitimizing deception. The reader does not see the ad in its usual form, but the text embedded in the author's stream, stylistically indistinguishable from the usual messages of the channel. This removes the natural alertness that usually accompanies the perception of advertising.

Another feature is equally significant: inside the Telegram, the appearance of mass support is extremely easy. In conditions when for a person the opinion of others serves as the most important guideline in a situation of uncertainty,

fraudulent networks actively reproduce artificial public evidence. This technology acts the stronger, the less opportunities for external verification a potential victim has. Positive reviews are published in the form of screenshots, voice messages, thanks, stories about "real results," photos of the alleged profit, emotional confessions of "students" and "participants." All this is presented as a spontaneous confirmation of the effectiveness of the service or the honesty of the organizers. However, upon closer inspection, it turns out that such materials are often fabricated, repeatedly reproduced in different channels, stylistically unified and included in a pre-calculated belief scenario. The researcher is presented not with spontaneous community opinion, but with a technologically constructed atmosphere of trust, in which the very multiplicity of "evidence" turns into a means of suppressing critical judgment.

Of particular danger is the placement of advertisements for dubious or frankly criminal services on the pages of outwardly respected authors. There is a stable mechanism of indirect trust in the public mind: if a well-known person, a popular publicist, an expert-looking commentator or a widely read author publishes a particular message, the audience is inclined to proceed from the assumption that at least a minimum conscientiousness check has already been made. Here the transfer of trust from the reputation carrier to the advertised object is formed. It is this transfer that becomes the decisive link, thanks to which a person takes a step towards a fraudulent scheme. He trusts not the proposal itself, but the symbolic capital that, as it seems to him, is behind the fact of publication.

In practice, such a check is often absent or purely formal. Moreover, the very logic of advertising turnover on messenger sites in some cases contributes to the systematic crowding out of due diligence by monetary interest. The reward for placement, the high speed of arrangements, the poor transparency of intermediary relationships, the ability to quickly remove a publication and the difficulties of subsequent proof create a situation in which a person with access to the audience is tempted to consider the advertiser not as a potential source of public danger, but exclusively as a source of income. This is how a morally and legally significant gray zone arises: the author of the channel may not be the direct executor of a fraudulent act, not enter into a direct conspiracy, and even subjectively not consider himself involved in the crime, but objectively he becomes a link in the legitimization of deception, without which the scheme would lose the most important resource - the initial trust of the audience. In a social sense, such mediation is not neutral. It gives deception the appearance of admissibility, and the criminal proposal - the aura of public acceptability.

Telegram is especially convenient for multilevel separation of roles between participants in a fraudulent network. This circumstance requires special attention, since it is it that turns disparate deception into a stable organized environment. One channel can act as a showcase and engage in primary attention. Another is to imitate educational activity by publishing texts of a

pseudo-analytical nature, giving the impression of theoretical thoroughness and professional depth. The third accumulates "reviews" and demonstrates supposedly independent evidence of performance. The fourth depicts a community of successful participants, where there is an atmosphere of involvement in a select circle and where success stories are constantly reproduced. The fifth pretends to be a support service, which is especially important for neutralizing doubts and removing anxiety in the late stages of involvement. Individual personal accounts play the role of mentors, curators, analysts, consultants, inspectors, representatives of the financial department and other figures, each of which is designed to strengthen the impression of organizational maturity and institutional reliability.

This distribution of roles has not decorative, but deep psychological significance. It gives the victim the impression that in front of him is not a narrow group of fraudsters, but an extensive social system with an internal division of labor, which in the eyes of an ordinary person is almost automatically equated with the sign of authenticity. The more roles, the stronger the sense that the activity is real; the more channels confirm each other, the less likely the thought of a single source of control seems. This forms a closed environment of mutual links, where each link refers to the other, and each confirmation looks outwardly independent. In reality, we are talking about a carefully built architecture of persuasion based on the principle of cross-legitimation. A person finds himself inside a space where all the elements say the same thing in different voices, and therefore a lie acquires persuasiveness not due to proof, but due to repeatability.

It should be emphasized that the strength of such a scheme lies not only in technical multichannel, but also in the consistent transfer of the victim from the zone of public visibility to the space of individual influence. It is here that one of Telegram's key advantages for fraudsters is revealed: the ease of transition from public communication to personal correspondence. The public channel performs the function of primary suggestion, forms interest, sets an emotional mood, creates a time deficit, promises access to an exceptional opportunity. However, the decisive impact often unfolds already in personal communication, where external witnesses disappear, where promises cannot be compared with the reaction of other participants, where pressure becomes targeted and continuous. In private correspondence, the fraudster adjusts the argument to a specific person, reveals his hopes, fears, level of financial literacy, degree of loneliness, risk appetite, need for recognition, desire for a quick improvement in life circumstances. The mass message here serves only as an input; genuine submission begins in individual contact.

This reorientation from public to personal space has colossal criminological significance. While the message is in the channel, it is at least potentially available to criticism, comparison, comprehension in collective mode. As soon as the interaction is transferred to a closed chat or personal correspondence, the

possibilities of public control are rapidly reduced. The victim loses external guidelines, and the fraudster gains an advantage in interpreting what is happening. He can explain delays, invent technical obstacles, create the appearance of escort, refer to security rules, promise an early benefit, demand additional payments and at the same time convince the victim not to disclose details. Closeness becomes not just a condition of convenience, but a structural element of criminal perception management. It is in it that lies receive the greatest freedom, since they do not meet an immediate external refutation.

The phenomenon of imitation of expertise, which in Telegram takes on especially convincing forms, cannot be ignored either. Visually and stylistically, the channel can easily reproduce the signs of a competent source: business tonality, a confident conceptual system, links to events in public life, graphs, reviews, "analytical" reasoning, imaginary professional comments, a narrative about complex mechanisms for making a profit or saving funds. For the mass addressee, such a speech sounds weighty precisely because it is saturated with terminology, categorical and emotionally disciplined. However, behind the external harmony of presentation often hides a meaningful emptiness, substitution of concepts or direct fiction. Imitation of knowledge is more important than knowledge itself, since its task is not to explain reality, but to suppress doubt. In this environment, pseudocompetence becomes an economic resource: the more convincing the speaker looks, the easier he translates the audience to actions beneficial to the scheme.

Therefore, it is necessary to see in Telegram not a set of isolated messages, but a special environment of social engineering, where the technical architecture of the site is combined with techniques of mass persuasion, psychological pressure and reputation mediation. There is no random heap of elements. Anonymity makes it easier to conceal genuine organizers. The speed of information dissemination allows you to instantly scale the lie. The multiplicity of channels creates an effect of diffuse but consistent support. Closed communities exclude external criticism and increase group pressure. Personal correspondence makes it possible to individually refine the script of deception. Advertising placements from respected authors provide the scheme with borrowed trust. Pseudo-educational and pseudo-expert materials give it an intelligent shell. Fabricated reviews form emotional validation. All together forms a holistic mechanism of submission of the victim, in which each link strengthens the other.

Therefore, the scientific description of this phenomenon cannot be limited to a superficial statement that fraudsters "use the messenger." Such a formula is too poor to convey the actual scale of the problem. This is a more serious process: about turning the digital environment into a space where trust is industrially produced, distributed and exploited. This is one of the most alarming features of modern fraud. If in previous forms deception often depended on personal contact, a one-time trick or a chance meeting, then in this case we are dealing with

a systemic organization of trust as a subject of criminal treatment. Trust doesn't come naturally here; it is constructed, heated, reinforced, confirmed and monetized. And the more invisible this process is to the victim, the more effective it is.

Hence the fundamentally important conclusion. The danger of Telegram in the context of fraudulent practices lies not in any one property, but in the synergy of many factors that, when combined, form an extremely favorable environment for deception. That is why the study should be aimed not only at identifying individual illegal ads or individual unscrupulous persons, but also at analyzing those social and communication mechanisms that make the fraudulent scheme convincing, sustainable and widespread. As long as this medium is perceived as a collection of private episodes, the temptation remains to underestimate its destructive potential. But in reality, we have an organized ecosystem of symbolic coercion, where lies are disguised as knowledge, advertising as recommendation, coordination as spontaneity, and criminal calculation as care for the user. That is why Telegram should be considered as one of the key objects of modern criminological, legal and socio-communicative analysis. Not because the site itself is exhausted by crime, but because it was within its limits that a new historical type of fraudulent influence was manifested with particular clarity: fast, multi-layered, reputationally mediated, psychologically accurate and therefore especially dangerous for wide sections of society.

A separate and extremely thorough consideration is required by the corpus of narratives devoted to the so-called staking programs, "freezing funds for the sake of income," "connecting to the internal remuneration of the network," as well as other forms of supposedly passive growth of digital assets. Already at the level of the conceptual apparatus, it is necessary to maintain increased rigor and legal restraint. It is unacceptable without sufficient evidence to assert the complicity of a specific site, settlement system, intermediary node or technical operator in the theft of user property. Such statements require not journalistic intonation, but a procedurally significant evidence base, including information about actual control over addresses, routes of movement of funds, the distribution of roles between participants in the scheme, the coordination of their actions and the presence of intent. However, it does not at all follow from this that a researcher, law enforcement officer or expert is obliged to refrain from more general and at the same time fundamentally important statements. It is quite permissible and scientifically necessary to point out otherwise: around the topic of "passive income" in the digital environment, an extremely favorable environment for abuse has developed, and the very design of the promised reward has become one of the most convenient masks for systematically misleading citizens.

The meaning of this environment is not only in the technical complexity of the relevant procedures, but above all in the special mode of perception in which the victim finds himself. He is offered not a simple transfer of funds to a third party

and not a direct call for dubious speculation, but an outwardly decent, almost bureaucratically ordered model of participation in a certain "internal mechanism" of the digital system. In the mind of a person, an idea is formed that he does not give property to unknown persons, but only temporarily transfers it to a special storage mode, confirmation of operations, maintenance of the computing infrastructure or other "official" purpose, for which the system allegedly naturally accrues remuneration. This is one of the key dangers: the criminal impact is disguised as a technological procedure, and the deliberately risky transfer of control over property is described in the language of neutral technical necessity.

Such a description is often based on semi-truths, which is its special destructive power. In digital settlement systems, there may indeed be mechanisms that reward participation in confirming operations, maintaining the stability of a distributed record, or other functional participation in the life of the network. But it is this limited, special and technically determined reality that serves as material for subsequent manipulation. Several terms are pulled out of it, freed from context, simplified to the limit, and then turned into a universal bait for the mass user. Scientific conscientiousness requires emphasizing: where a person does not understand the legal regime of the transferred property, does not control the procedure for blocking and unblocking it, cannot verify the source of the promised profitability, does not have the ability to independently verify the authenticity of the technical procedure and is forced to rely entirely on the words of the intermediary, there the space of civil circulation is rapidly turning into a space of criminogenic risk.

It is especially significant that abuses in this area are built not on one, but on several mutually reinforcing forms of substitution. The user may be offered "official" or "semi-official" forms of participation, externally correlated with a known site, calculation environment or a common digital asset. The similarity of names is used, color schemes are repeated, emblems are imitated, payment pages are stylized, the vocabulary of notifications and service messages is reproduced. False escort accounts are created, depicting relief service representatives, community treasurers, reward distribution curators, technical administrators. Addresses for transferring funds are replaced at the stage of correspondence or copied in such a way that the victim does not notice the replacement of one or more characters. Imaginary calculation windows and fake income accrual interfaces are constructed, in which the growth of the balance is displayed as a fait accompli, although in fact there is only a visual decoration in front of the user that is not related to any real property law. In other words, the victim is immersed in an artificially created environment of plausibility, where each individual detail may seem insignificant, but their entire totality acts with the accuracy of a well-built persuasion mechanism.

Here it is necessary to emphasize: not only technical falsification as such is crucial, but also the consistent destruction of the victim's ability to distinguish between the levels of legal and factual reality. For an unprepared person, the line between the legitimate functionality of the site, a dubious intermediary service and outright theft turns out to be not just unclear, but deliberately blurred. It is the intentionality of this blur that deserves special attention. We are not talking about spontaneous confusion arising from the complexity of new settlement mechanisms, but about the targeted use of such complexity as an instrument of criminal influence. The less distinguishable the legal statuses of the participants, the more vaguely distributed the powers, the thicker the fog of terms and pseudo-technical explanations, the easier it is to persuade a person to transfer property without leaving him with the feeling that he is entering into a dangerous or illegal attitude. Blurring borders becomes not a side effect, but the main method of theft.

In the scientific description of these practices, it is especially important to show that the promise of income here performs not only an incentive, but also an exculpatory function. The victim is informed that the temporary unavailability of funds is a sign of the seriousness of the procedure; that the inability to immediately withdraw assets is due to an "internal retention period"; those additional transfers are required for "confirmation of status," "activation of accruals," "unblocking of remuneration," "admission to increased coefficient." Thus, each subsequent extraction step is provided with a language cover in advance. If the initial translation can still be perceived as risky, then subsequent transfers are already submitted as an inevitable continuation of the previously begun, supposedly legal procedure. The victim is drawn into a chain of self-foundation, where the recognition of deception psychologically becomes more and more difficult, and therefore the likelihood of new transfers, contrary to common sense, increases.

No less significant is the fact that such schemes flourish not in airless space, but in an environment of instant correspondence, where the speed of communication, the multiplicity of communication channels and the dispersion of responsibility create truly exceptional conditions for cybercriminals. In the messenger environment, another feature of modern criminal networks is especially pronounced - their ability to merge property encroachment with a stable system of information influence. Before us is no longer a single act of deception in its classical form, but a complex socio-psychological construct in which theft is provided not only by a false fact, but also by a whole worldview framework. A person is sold not just a service, not just participation in a dubious mechanism and not just hope for income. He is sold a picture of the world.

This picture of the world is built according to the laws of quasi-religious mobilization of consciousness. Traditional financial institutions are declared archaic and doomed; government regulation is portrayed as impotent, belated, or fundamentally incapable of understanding new forms of value conversion; law

seems heavy and alien to the "new reality"; caution is branded as ignorance; doubt - as a manifestation of mental retardation or a missed historical opportunity. On the contrary, those who have already "entered the system," "understood the era," "managed to join," appear in the role of initiates, seeing what is hidden from the majority. This creates the most dangerous cult of chosenness, in which trust is transferred from institutions, verifiable procedures and formal guarantees to the figures of self-appointed guides, mentors and "those who have already earned."

It should be pointed out with all certainty that such rhetoric is not a simple advertisement in its usual economic sense. Advertising seeks to distinguish a product, service or market participant from competitors; the ideological shell of the crime strives for something else - for the preliminary disarming of criticism. She is proactive. Even before the victim has questions about the legal status of the intermediary, the source of profitability, the distribution of risks, the procedure for storing assets, the jurisdiction of the dispute, the limits of liability and the technical verifiability of operations, he is already being told that all such questions come from "outdated thinking." Even before he turns to a lawyer, a settlement specialist or a representative of a legal platform, they explain to him in advance that the "old institutions" do not understand anything in the "new era." This is not an accompaniment to deception, but its preliminary strategic provision.

Hence the special public danger of the practices in question. They encroach not only on the property of a particular person, but also on the very ability of a citizen to navigate the criteria of reliability, legality and provability. When deception is systematically framed as progressive knowledge, and violation of the elementary rules of property caution is presented as a sign of intellectual courage, not one victim is already at risk, but the foundation of public trust in law as a form of reasonable streamlining of relations. Crime seeks to impersonate historical inevitability. This is where his particular cynicism lies. Embezzlement masquerades as the future, and criticism of this embezzlement as backwardness.

It is fundamentally important for a scientific journal to record: the more intensively the criminal environment resorts to the motives of the "new economy," "internal remuneration," "digital freedom," "avoiding intermediaries" and "income without effort," the more urgent the requirement for strict delineation of facts, assessments and evidence becomes. You cannot replace research with a slogan, but you cannot pretend that we have a morally neutral dictionary of technological innovations. The external neutrality of the terms often hides a well-verified system of psychological capture: first, a person is promised access to exceptional knowledge, then they are involved in a not fully understandable procedure, after which they replace the legal analysis with emotional loyalty to the community, and in the final they use the already formed dependence on their own mistake. This is how a vicious circle of criminogenic trust is formed, where each new doubt is suppressed by reference to previous

investments, to the imaginary growth of the balance sheet, to the evidence of dummy participants and to the fear of being the one who "could not stand it to the end."

In this context, exploratory caution must be coupled with rhetorical clarity. Unfounded accusations against specific sites should be avoided if there is no verified information about their direct involvement in theft. But it is equally unacceptable to soften the obvious: the sphere of the promised passive growth of digital assets has become one of the most convenient fields for exploiting gullibility, legal ignorance and psychological vulnerability of citizens. Here they parasitize on the complexity of calculation mechanisms, on the lack of special knowledge, on the authority of visual similarity, on the habit of trusting the "official" tone of correspondence and on the deep desire of a person to believe that income can be simultaneously high, stable, easy and practically risk-free. It is this combination of promise, nebula and pseudocompetence that makes the environment in question so dangerous.

Therefore, a qualified analysis of such practices should proceed from the fact that we are not facing a set of random episodes and not just a series of everyday deceptions in a new technical design. Before us is a special type of criminal communication, in which the terminology of digital calculations is combined with techniques of symbolic imitation, emotional infection, fake authority and ideological suggestion. Its purpose is not only to seize property, but also to preliminarily destroy those internal protective mechanisms, thanks to which a person usually distinguishes verifiable from unverifiable, legal from dubious, professional advice from obsessive agitation. Where the very ability to distinguish is destroyed, theft becomes almost invisible until the loss of property becomes irreversible.

That is why the phenomenon under consideration should not be described as an exotic consequence of technical progress, but as a natural result of the combination of three forces: the high complexity of the digital environment, the low legal and financial training of a significant part of users and the aggressive adaptability of criminal networks that can clothe old forms of theft in the latest verbal and visual shells. One of the most disturbing forms of modern property encroachment is born in this compound. Her danger is greater the more convincing she speaks in the language of novelty, freedom and chosenness. And if science, law and society do not learn to recognize this shell in all its rhetorical and technological sophistication, then the crime will continue to come to a person under the guise of education, income and familiarization with the future. This is the main conclusion: the ideologization of deception today has become not an external decoration of the criminal scheme, but its internal bearing frame.

Social engineering in an elite shell: offices, security, public speaking and the cult of respectability

One of the most disturbing and at the same time the least correctly recognized trends in modern crime is a deep transformation of the very appearance of fraudulent activity. If before the public imagination associated deception mainly with the underground, with untidy conspiracy, with emphasized secrecy and obvious illegality, now a significant part of criminal schemes is built on the exact opposite principle. Modern fraud is increasingly seeking not to hide signs of decency, but to appropriate them for itself. It does not avoid external forms of order, but carefully reproduces them; does not repel a potential victim with rudeness and chaos, but, on the contrary, surrounds it with an atmosphere of business, organization and seeming legitimacy. This is one of the most important features of the current stage of development of deceptive practices: criminal intent is masked not by the lack of institutional signs, but by their demonstrative excess.

That is why fraudsters rent solid premises in business parts of the city, are located in buildings with well-groomed entrance groups, guarded entrance, reception areas, meeting rooms, signs, internal admission rules and other external attributes of a sustainable organization. The internal space of such structures is often built with amazing thoroughness: secretaries meet the visitor, an appointment is made, unified forms are used, certificates, certificates, permits are located on the walls, sometimes images of state symbols, excerpts from legislation, schemes of supposedly transparent activities. Employees answer the phone in an even, confident voice, avoid fuss, demonstrate proficiency in professional terminology, and act according to a pre-worked scenario. All this creates not just a favorable impression, but a special psychological environment in which the visitor gradually develops a feeling of institutional reliability. A person begins to trust not the content of the activity, but its external production.

This is the main calculation. For a significant part of citizens, external order is still one of the strongest grounds for trust. This circumstance has deep socio-psychological roots. In everyday life, a person is forced to constantly resort to simplifying signs of assessment: he cannot each time conduct a full-fledged legal, financial and organizational audit of each counterparty, and therefore relies on external signals that are traditionally associated with legality and good faith. A good building, security at the entrance, a neat interior, a consistent style of communication, an orderly workflow, the presence of seals, certificates, official designations - all this is perceived as confirmation of the seriousness of intentions. Meanwhile, this perception is based on a dangerous mixture of form and essence. The presence of an office proves only the presence of an office; the presence of protection proves only the presence of protection; the presence of a business ritual proves only the ability to reproduce it. None of these circumstances in itself confirms the legality of financial transactions, the validity

of permits, the authenticity of the declared type of activity, the transparency of internal procedures, the reliability of reporting and, finally, the absence of a criminal intent.

Moreover, it must be emphasized that external respectability in the cases under consideration is often not a side sign, but a central tool of the crime. She performs the function of psychological disarmament. A potential victim, finding himself in a space of emphasized order, ceases to expect danger where it is actually concentrated. Fraud of a new type acts not contrary to trust in social institutions, but parasitizes on it. It uses a deeply rooted attitude among citizens: if the activity is so clearly and calmly carried out in plain sight, if it is accompanied by the usual signs of business life, then it is already checked by someone, admitted, recognized and, therefore, does not pose an immediate threat. It is this logic that turns out to be deadly vulnerable. The criminal does not destroy the usual reliability criteria, but replaces them with meaningfully empty, but impressive shells.

Of particular danger is the fact that such an imitation of legality operates at several levels of perception at once. Firstly, it affects visually: premises, clothes, furniture, documents, signs, office offices, office equipment create a material picture of a sustainable business. Secondly, it acts in a speech way: measured intonation, legally colored formulations, references to the procedure of work, internal regulations and imaginary requirements of the law give the conversation the appearance of competent professional communication. Thirdly, it acts through social imitation: a person sees other visitors, employees, assistants, sometimes a purposefully created queue, hears business negotiations, observes the appearance of intensive work and concludes that he is really a functioning organization. Fourth, she uses the time factor: the victim is given the opportunity to gradually get used to space and faces so that trust does not arise instantly, but as if naturally and independently. The more natural it seems to a person that trust has arisen, the more difficult it is for him to admit that this trust was provoked and calculated in advance.

In scientific and practical terms, we should talk about the purposeful construction of false institutional legitimacy. The criminal group seeks not only to offer the victim a disadvantageous or fictitious transaction, but also to embed this transaction in the decoration of legitimate economic turnover. Thus, deception acquires a qualitatively different stability. If primitive falsehoods can be exposed by a single clarifying question, then falsehoods surrounded by many agreed-upon outward signs resist questioning for considerably longer. It is psychologically difficult for a person to doubt everything at once: indoors, and in documents, and in the manner of communication, and in the behavior of employees, and in the formal openness of activities. The scale of the staging begins to be perceived as evidence of authenticity, although in reality it can only be evidence that the crime was prepared in advance and carefully prepared.

No less significant component of this trend is the public activity of persons involved in such schemes. Their participation in forums, round tables, conferences, industry meetings, expert discussions and other public events dedicated to the turnover of digital assets and related financial relations creates a halo of recognition and admissibility around them. Appearance on the stage, presence at the exhibition place, inclusion in the discussion, proximity to the microphone, mention in the program of the event, photographing with other participants - all this produces a powerful symbolic effect. Public presence begins to be misperceived as an implicit affirmation of good faith. For a wide audience, participation in a professional discussion often means belonging to a legitimate industry, although in reality there is no automatic connection between public visibility and legal purity of activity.

This transition from the figure of a suspicious subject to the figure of an "industry representative" is extremely dangerous. He destroys the basic instinct for caution. The potential victim disappears the natural protective question: if the criminal is in front of me, why is he acting so openly, so confidently, so demonstratively not hiding? But it is here that a new level of cynicism of modern deception is revealed. Openness is used as a mask of immunity. The calculation is based on the fact that an ordinary person is inclined to consider publicity as the opposite of crime, when in reality publicity can be only one of the tools for covering it. Moreover, openness in such cases takes on the character of an offensive strategy: the more noticeable the subject in public space, the stronger it seems that he has nothing to hide and that the very appearance of accessibility already excludes the criminal nature of the activity.

It should be especially noted that participation in public events performs several functions at once. It provides social "whitening" of reputation, forms a circle of potential clients and trusted intermediaries, makes it possible to refer to one's own fame, creates an archive of visual evidence of apparent respectability, and, finally, connects the criminal with a wider professional field in which he begins to be perceived not as an exception, but as one of many actors. In the future, these images, videos, mentions in programs and lists of participants are used in negotiations with new victims as confirmation of the allegedly recognized status. The very fact of presence on a public platform turns into a surrogate for reputation, although this presence, as a rule, does not mean any real verification of the legality of activities.

This reveals an important societal paradox. In normal civil circulation, openness, public reporting, participation in professional discussion and readiness for communication can indeed be considered as positive signs. However, in a more complex criminal environment, the same signs no longer have the same self-evident evidence. Criminal actors have learned to appropriate not only the language of legality, but also its rituals, not only symbols of competence, but also mechanisms of social recognition. This leads to a fundamentally important

conclusion: neither external orderliness nor public visibility can any longer be considered sufficient grounds of trust. Where earlier it seemed to a person that he sees a guarantee of reliability, today he often sees only a more skillful form of disguise.

What has been said requires a broader social understanding. Before us is not a private technical technique of individual criminals, but a symptom of a dangerous shift in the culture of deception. If the previous forms of fraud were built mainly on direct lies and concealment, then new forms are increasingly based on the dramatization of legality. The criminal ceases to look like a troublemaker; he strives to look like his spokesman, and sometimes like his zealous protector. He talks about legal regulation, about transparency, about reliability, about protecting the interests of clients, about compliance with procedures. He can refer to the development of new financial relations, the complexity of the legal environment, the need for professional mediation. And the more convincingly he reproduces these speeches, the more difficult it is for a layman to distinguish awareness from manipulation, competence from acting, legitimacy from her stage imitation. The most dangerous today is not the deception that looks like a deception, but the one that looks like an exemplary order.

That is why opposition to such practices cannot be limited to calls for general vigilance in their superficial, everyday understanding. We need a consistent reassessment of the trust criteria themselves. A citizen must proceed from the fact that the premises, security, reception, official clothes, confident speech, participation in the conference, photographs from public events, references in the business environment and other signs of external recognition are not evidence of legality, but only circumstances requiring additional verification. The legal status of the organization should be established not by the interior, but, according to reliable information, from official sources; availability of permits - not by copies on the wall, but by their reality and volume; financial reliability - not on the impression of negotiations, but on the structure of operations, documented responsibility and real verifiability of obligations. Trust must shift from form theatre to substance testing.

Ultimately, we are talking about protecting not only the property interests of citizens, but also the very ability of society to distinguish between true institutionality and its criminal imitation. Where a fraudster freely puts on a mask of respectability, it is not an individual victim who is at risk, but public trust as such. Each such case destroys confidence in the value of external signs of order, undermines the authority of conscientious participants in the turnover, enhances the atmosphere of general suspicion and, which is especially dangerous, normalizes the idea that a decent appearance can be just a kind of criminal toolkit. This is no longer just private deception; it's undermining the very social fabric of trust. Therefore, exposing such mechanisms is not an

optional task, but an urgent duty of legal science, law enforcement practice and public education. As long as society continues to unconditionally believe the facade, the facade will remain one of the most profitable instruments of crime.

Why wealthy and outwardly rational people become victims

The conventional wisdom that a naive, inexperienced and poorly educated person becomes a victim of fraud is not just wrong - it is socially dangerous. Such an idea distorts the very nature of the criminal impact, replacing a serious conversation about the psychological mechanisms of deception with a convenient and soothing myth. While a person is convinced that criminals hunt exclusively for gullibility in its rude and obvious form, he does not notice a much more significant circumstance: fraud affects not only weakness, but also strength; not only ignorance, but also confidence; not just poverty, but well-being. This is one of the most insidious features of modern criminal schemes. They are aimed not at the abstract "stupidity" of the victim, but at the universal properties of human consciousness - at the desire for consistency, at faith in one's own ability to recognize a threat, at the desire to preserve dignity, position and control over what is happening.

That is why socially prosperous, wealthy, professionally successful people often turn out to be not a random, but a priority goal for the organizers of complex fraudulent constructions. This is not about a paradox, but about a pattern. Where funds, reputational capital, broad connections, the habit of independent decision-making and the conviction of one's own competence are concentrated, a particularly favorable environment arises for the offender. Outwardly, such a person looks protected: he has experience, education, access to information, often occupies a responsible position, knows how to negotiate and is used to assessing risks. However, it is these qualities that can be turned against him under certain circumstances. The fraudster does not break the personality with brute force; he makes her work against herself. He doesn't always demand immediate compliance. On the contrary, it gives the victim the feeling that he is acting freely, reasonably, prudently and even with benefit for himself.

The special attractiveness of a wealthy person for a criminal is primarily determined by the fact that he has a resource for repeated extraction of funds. Unlike a one-time theft from a random victim, the impact on a financially prosperous victim can be built as a long process, sequentially unfolding in time. Withdrawals in such cases are rarely limited to one transfer, one transaction or one assignment. On the contrary, the criminal scheme is often organized as a chain of logically related demands, each of which seems to be a continuation of the previous one and therefore is not perceived as a final catastrophe. First, relatively moderate participation is proposed, then there is a need to "confirm the seriousness of intentions," then - "consolidate the achieved result," "protect the invested," "complete the procedure," "eliminate the obstacle that has arisen." This is how a gradual retraction develops, in which a person loses funds not

simultaneously, but in portions, each of which, against the background of what has already been invested, begins to seem psychologically permissible. The more resources the victim has, the longer the offender is able to maintain the illusion of reversibility of the situation and the wider the field for re-recovery of money becomes.

But material resource is only one side of the issue. No less important is the psychological attitude inherent in many people who have reached a noticeable social position. Such persons often really have a high degree of personal composure, professional discipline and practical insight. They are used to making decisions without outside care, navigating difficult circumstances, being responsible for the consequences of their actions. This quality is valuable in itself, but in conditions of criminal influence, it can give rise to dangerous self-confidence. The harder a person is convinced that it is difficult to deceive him, the less attention he pays to the early signs of manipulation. It does not correlate itself with the image of a "typical victim," and therefore often does not include internal mechanisms of alertness where it is especially necessary. In other words, vulnerability arises not from a lack of intelligence, but from excessive trust in one's own protective abilities.

There is a subtle, but extremely important psychological law. A person who considers himself competent tends to perceive his own first impression as especially reliable. If the interlocutor speaks confidently, speaks professional vocabulary, maintains the proper tone, demonstrates knowledge of social codes and skillfully reproduces signs of legality, then the critical check may weaken. The victim does not say to himself: "I believe without reason." He tells himself something different: "I know how to distinguish serious from frivolous; since this does not cause me doubts, it means that the situation is controlled." This is how one of the central illusions of fraudulent influence arises - the illusion of personal control. A person is convinced that he does not become an object of someone else's will, but makes his own balanced choice. This is exactly what the criminal needs: not to suppress resistance openly, but to dissolve it in the feeling of rationality of what is happening.

Of particular importance for a socially prosperous audience are signs of exclusivity and status. For many wealthy people, not only money as such is essential, but also forms of handling them, emphasizing a special position: closed access, special service procedure, personal support, not open opportunities for everyone, confidential conditions, resolving the issue outside of general procedures. In this area, criminal influence becomes especially sophisticated. The fraudster rarely acts as a rude obsessive supplicant. In contrast, it creates an atmosphere of respect for the position of a potential victim. He does not "draw in" - he seems to admit. Does not "persuade" - but "provides a rare opportunity." Not "presses" - but "trusts." This intonation substitution has tremendous power. A person begins to perceive contact not as a suspicious proposal from the outside,

but as a sign of recognition of his own level, competence and belonging to a special circle.

That is why the rhetoric of exclusivity is so often present in complex criminal schemes. The victim is told that he is not facing a massive offer, but an individually addressed opportunity available to few. Closeness, chosenness, special admission, personal recommendation, respect for status, the need to observe silence and delicacy are emphasized. All this serves a double function. On the one hand, a person is flattered by the consciousness of his own isolation. On the other hand, exclusivity itself begins to justify the absence of conventional verification procedures. If something is presented as rare and intended for "their own," then the lack of transparency no longer seems an alarming sign, but, on the contrary, is perceived as a natural property of the privileged order. Where there should be doubt, there is a sense of involvement. This is the power of status manipulation: the criminal does not exploit vanity in its superficial form, but the deep need of a person to see confirmation of his own significance.

Among the most destructive mechanisms is the so-called cost trap, which often takes on particularly severe forms among wealthy people. Its essence lies in the fact that a person continues to support a deliberately unfavorable, and sometimes clearly disastrous line of behavior only because too much has already been invested in it. In everyday consciousness, such behavior is often explained by "greed" or "recklessness," but this explanation is superficial and unfair. In reality, we are talking about a complex internal conflict between the recognition of a mistake and the desire to preserve a holistic image of one's own personality. When significant funds have already been contributed to the scheme, it is difficult for a person to accept the idea that all this was not an investment, not a calculation, not a strategy, but the result of a criminal deception. Recognition of fraud does not only mean fixing property damage; it is experienced as a blow to self-esteem, to the idea of one's own maturity, experience and ability to see through people.

For a socially prosperous victim, this problem is aggravated by the fact that a reputation factor is almost always woven into the case. Losing money is hard, but for many it is even harder to allow the possibility of moral and social humiliation. If a person is used to taking the position of an adviser, leader, connoisseur, person whose opinion is listened to, then the recognition of one's own vulnerability is especially painful. He begins to save not only capital, but also a symbolic image of himself. At this point, the criminal scheme moves from the field of financial encroachment to the field of personal enslavement. Each new transfer of funds, each attempt to "rectify the situation," each consent to the next condition can be dictated not by the hope of profit as such, but by a desperate desire not to see oneself in the role of a deceived person. Paradoxical, but natural is the fact that it is a strong personality, accustomed to being responsible for his decisions,

sometimes resists for a particularly long time to admit that he has become a victim of someone else's manipulation.

Secrecy from family, colleagues and business partners further strengthens the power of the criminal structure. The fewer people are devoted to what is happening, the narrower the space for external correction of delusion. The fraudster is almost always interested in ensuring that the interaction with the victim is as isolated as possible. Sometimes this is achieved through links to confidentiality, sometimes through an appeal to a special trust, sometimes through suggestion that disclosure can "disrupt a profitable opportunity" or "cause unnecessary complications." But regardless of the form, the result is the same: a person is left alone with a skilfully organized version of reality. Where there is no external view, the internal error quickly turns into a closed system. This is especially dangerous for those who, for reasons of status or pride, are already inclined not to bring their doubts to the discussion.

This makes it clear why some victims continue to send money even after obvious alarms appear. To an outsider, this behavior may seem inexplicable. However, it becomes clear if you see the totality of the existing factors: material resource, confidence in one's own competence, attachment to status signs, a gradual increase in investments, fear of reputational damage, isolation from a critical environment, unwillingness to recognize a painful truth. A person continues to act not because he does not see the danger at all, but because recognizing the danger requires too high an internal price. At some point, the choice is no longer experienced as "send or not send money," but as "maintain hope for recovery" or "immediately recognize a heavy defeat." The psyche, seeking to avoid a destructive blow to the sense of self, often chooses to extend the illusion. So the fraud feeds not on the victim's blindness, but on her painful attempt to protect the remnants of the internal order.

Consequently, the prevention of such crimes cannot be built on a condescending contrast between "smart" and "stupid," "successful" and "simple-minded." This approach is not only scientifically untenable, but also practically destructive. It forms a false sense of invulnerability in those who consider themselves to be among the "unsuitable" victims, and increases shame in those already affected, preventing timely seeking help. Meanwhile, effective prevention should proceed from the exact opposite understanding: almost any person can become a victim of complex fraud if the offender correctly selects the form of influence to his values, experience, vulnerabilities and self-image. For one, fear becomes a bait, for another - trust in authority, for the third - hope for a rare opportunity, for the fourth - a desire to save face. There is no universal invulnerability.

Therefore, it is especially important to change the very public language of the conversation about fraud. It is necessary to abandon the contemptuous intonation with which the victims are often discussed, and replace it with an accurate, sober, psychologically competent analysis. A deceived person is not a

caricature figure or an object for ridicule. Very often he is a person with a high level of education, significant life experience, a stable social position and a developed sense of responsibility. That is why his defeat should not be perceived as a curiosity, but as a serious public signal. If a criminal is able to convince even a trained, disciplined and prosperous person, then the problem is rooted not in private "stupidity," but in the systemic power of fraudulent influence. And until this is fully recognized, prevention will remain superficial, and many people - without the necessary internal protection.

Ultimately, the main truth is this: fraud wins not when it meets exclusively ignorance, but when it skilfully adapts to human dignity, vanity, responsibility, hope, fear and the desire not to lose control. It enters not only through the door of weakness, but also through the door of strength. This is his true danger. And therefore, society must learn a tough, but necessary conclusion: the higher the social position of a person, the stronger his confidence in his own prudence, the more significant his reputation rates, the more attentive he should be to the risk of becoming an object of complex criminal deception. Only the rejection of soothing myths, only the recognition of universal human vulnerability to finely structured manipulation creates the basis for truly effective prevention and timely assistance to those who are drawn into a destructive scheme.

Exit from destructive groups and manipulation chains

One of the most painful questions for victims and their loved ones is how to get a person out of a state of dependence on a fraudulent group if he is already emotionally involved, continues to believe the "mentor" and rejects the family's arguments. Rough pressure must be abandoned here. Direct accusations, ridicule, humiliation, shouting and categorical demands to "immediately come to your senses" often backfire. A person already bound by shame and hope perceives pressure as a threat to the last source of meaning and becomes even more dependent on criminals.

The first step is to end the immediate impact channel. This does not always mean a complete and abrupt disconnection of communication if it is not possible. But it is necessary to at least temporarily stop transfers of funds, the issuance of classified data, the implementation of instructions, the installation of programs and communication in conditions of urgency. The main task is to return time to the victim. Fraud lives by acceleration; defence starts by slowing down.

The second step is the restoration of external reality. It is important for the victim not to read morals, but to help check the facts: the legal status of the site, the validity of addresses, the history of the domain, the presence of independent references, signs of mass complaints, inconsistencies in documents, the lack of confirmed withdrawal of funds. When criticism relies not on general words, but on specific verifiable facts, the chances of restoring criticality increase.

The third step is the removal of paralyzing shame. A person needs to say bluntly that highly intelligent, organized schemes are designed for normal mechanisms of the psyche and that the fact of falling into them does not mean stupidity or moral inferiority. As long as the victim feels humiliated, he will not protect the scammers, but the remnants of his own dignity - and thereby unwittingly remain on their side.

The fourth step is to divide the problem into levels. It is necessary to separately discuss the stolen funds, separately - the psychological state, separately - legal actions, separately - digital security. When everything mixes into one lump of horror, a person falls into a stupor. When the problem is decomposed, it becomes possible to act consistently: save evidence, notify the bank, change access, disable malicious permissions, collect correspondence, seek legal advice, and limit new contacts with the scheme.

The fifth step is to help loved ones without assigning control. If relatives completely take away the right to vote from a person, he can secretly return to the scammers, since they will seem to him the only ones who "understand" him. Joint decision-making is much more effective, in which the victim retains subjectivity, but receives a protective circuit and external verification.

In severe cases, psychological help is needed, especially if the victim has developed insomnia, anxiety, panic reactions, obsessive re-reading of correspondence, appetite disorders, a feeling of complete life collapse or suicidal thoughts. In such situations, a financial crime ceases to be only a property episode and turns into a traumatic event that affects the whole person.

Why refunds most often do not work in practice

One of the most painful topics in the discussion of crimes related to the theft of funds and digital property values is the question of their return. It is in this place that not comforting rhetoric is needed, not trading in false hope, but utmost scientific and moral honesty. A dangerous delusion still lives in the mass consciousness, as if after the discovery of deception there is some understandable, almost mechanical way to restore the lost property status: it is enough to turn to "knowledgeable people," submit a "correct application," send a "special request," and the stolen will be returned. However, the real law enforcement, technical and organizational picture is much harsher. In the vast majority of cases, promises of an easy, quick, or even more so guaranteed return of stolen funds do not correspond to reality. Moreover, a whole parasitic layer of secondary abuse has developed around the victim's figure: a person who has already experienced property loss, psychological shock and undermining trust is often re-involved in deception already under the guise of "return specialists," "international legal intermediaries," "transaction analysts," "representatives of supervisory authorities" and other imaginary saviors.

This state of affairs requires not only description, but also fundamental understanding. The low practical effectiveness of the return of stolen funds is explained not by one reason, but by the totality of the circumstances of the technical, legal, organizational, evidentiary and psychological order. If this totality is not fully revealed, society is doomed to constant reproduction of false expectations, and therefore to new waves of disappointment, distrust and re-victimization. The question here is not only about money as such. It concerns the very ability of the law and the state to respond to the challenges of the new criminal environment, in which the speed of movement of assets, the blurring of territorial borders and anonymizing mechanisms are often ahead of traditional forms of response.

The first fundamental reason is the technical and jurisdictional fragmentation of the movement of funds. Modern thefts are rarely limited to simple linear transfer from victim to attacker. On the contrary, the criminal scheme is built in such a way that already in the first minutes after receiving the funds it is difficult to identify them, divide the flow into many parts, direct it through chains of addresses, intermediate accounts, exchange nodes, settlement intermediaries, decentralized protocols, over-the-counter exchanges, nominal holders and services located in different states or deliberately avoiding a certain territorial binding. As a result, in the face of the law enforcement officer, there is not a single object of recovery, but a dispersed network of movements, where each next section of the chain can be regulated by a different national law, different standards of personal identification, different deadlines for responding to requests and other grounds for blocking.

This fragmentation is not abstract, but extremely practical. Even if the movement of assets is partially traced, the traceability itself is not yet identical to the possibility of return. Setting a route does not mean getting a stop lever. You can see how the stolen funds are crushed, mixed with other property masses, transferred to other forms of property value, passed through conversion services, distributed among many addresses or displayed on sites that are not interested in quick and meaningful interaction with the victim or the investigation. Each such link increases not only the technical complexity, but also the time distance between the moment of theft and the chance of effective intervention. And time in such cases is almost fatal: the faster the property trace dissipates, the weaker the likelihood of the actual seizure or freezing of assets.

Jurisdictional multiplicity exacerbates the problem. A request for assistance may require compliance with complex international procedures, translation of documents, confirmation of the applicant's procedural status, passing through interdepartmental channels, waiting for formal answers, and sometimes overcoming direct refusal to cooperate. The offender, on the contrary, acts in a different time mode: several minutes or hours are enough for him to build a chain of movements, the consequences of which will unravel for months. This reveals

a painful gap between the instantaneity of the criminal action and the slowness of the institutional response. It is this gap that forms one of the key reasons why the hope of a subsequent miraculous refund so often turns out to be an illusion.

The second reason is due to the irreversibility of a significant number of operations. In the traditional banking environment, a citizen has developed the idea that a disputed payment can be canceled, withdrawn, challenged, blocked or returned if there is a statement, confirmation of fraud and participation of a credit institution. But in the field of digital property values, many translations, after their proper confirmation, do not have the property of simple reversibility. The technical record records the fact of the executed order, and if the operation has received confirmation in the relevant accounting system, its subsequent cancellation, as a rule, is not the usual procedure. What is perceived by the victim as an obvious injustice, from the point of view of technical fixation, often looks like a completed and formally correct expression of will.

This conflict between material truth and technical form is especially tragic in cases where the victim himself, under the influence of deception, psychological pressure, false urgency or artificially created trust, approved a harmful action: entered the confirmation code, signed the transaction, provided access to the account, independently sent funds to the specified address, agreed to install remote control programs, transferred money allegedly for "verification," "defrosting," "identity confirmation" or "ensuring a safe transfer." From a human, moral and criminal-legal point of view, we have deception and theft. But from the standpoint of a dry technical record, the operation often looks like a voluntarily confirmed one. This does not destroy the fact of the crime, but sharply complicates the dispute about the return, since there may be no formal signs of forced write-off.

It is here that the limitations of everyday thinking become especially obvious, according to which any injustice automatically entails a simple restoration of the previous situation. The law requires proof, the technique fixes the form of action, the sites assess compliance with their regulations, and the investigation needs a specific evidence base. Where the victim was misled but personally confirmed the operation, the space for immediate challenge is substantially narrowed. Therefore, slogans about "one hundred percent return" in such situations are not just professional dishonesty, but the actual use of legal illiteracy and emotional vulnerability of a person.

The third reason is the limited and institutional focus of the reaction of the sites through which the stolen assets could pass. In public perception, a large exchange, exchange or settlement platform is often presented as a natural ally of the victim: if assets have appeared somewhere, then they can be immediately blocked and returned to the owner. But such a picture is overly simplistic. Any site operates primarily within its own internal rules, contractual terms, identification procedures, standards of interaction with authorities and risk

management policies. Its primary task is not to restore the property status of a particular citizen as such, but to comply with its own regulations, minimize its own responsibility, prevent abuse of the site itself and fulfill the mandatory requirements of the jurisdiction in which it operates or with which it is associated.

From this follows an extremely important conclusion: even the presence of a well-known site in the criminal chain in itself does not mean a high probability of return. Firstly, assets can only be there for the shortest possible time, after which the attacker manages to withdraw them, exchange, redistribute or convert them into another form. Secondly, blocking often requires not an emotional story of the victim, but a clearly formalized appeal, identification of the controversial operation, confirmation of the applicant's connection with the stolen funds, and sometimes an official request from the authorized body. Thirdly, even with the conscientious behavior of the site, its reaction is limited by the actual presence of assets in the accounts or addresses under its control. If funds have already been withdrawn by the time the appeal is considered, the legal and technical possibility of impact may be lost.

It is especially dramatic that the window for a real lock is often not weeks, but hours, sometimes minutes. Meanwhile, the victim often does not immediately realize the fact of theft. First, he is kept in a state of false hope, they promise profit, convince him of the need for additional actions, create the illusion of a temporary technical delay, refer to the "security service," "financial control," "tax audit" or "international transfer." As a result, time is running out exactly when it is most valuable. By the time a person finally realizes that he has become a victim of a crime, the property trace can already be so scattered that even the most conscientious intervention will not give a practical result.

The fourth reason is insufficient, fragmented and untimely evidence. This circumstance is often underestimated in scientific and applied terms, although it becomes decisive in many cases. A victim going through shock, shame, guilt or fear of publicity often seeks help late. Often, he deletes correspondence, believing that in this way he gets rid of traumatic reminders; Clears the call history. loses access to used accounts; does not save screenshots; does not capture recipient addresses; does not record the sequence of their actions; does not remember from which device, at what time and through what service he made transfers; cannot recover which confirmation codes entered and which permissions granted. In some cases, the transfer is carried out from several devices, through different accounts, when changing the network connection, using one-time communication channels or temporary identifiers. All this makes the actual picture blurred precisely when maximum detail is required for a successful response.

For law enforcement agencies, courts, representatives of sites and other participants in the process, it is not the general conviction of the victim that he

was deceived those matters, but the totality of specific, verifiable, comparable data. The questions will always be the same: who communicated with whom, in what way, at what time, through what communication channels, what details were used, to which addresses or accounts the funds were transferred, what promises were made, what actions were confirmed, what documents were preserved, what event logs can be requested, on which device there are traces of access, what is the sequence of operations and which of them relate to each other in time. Where there is no evidentiary density, the legal position is exposed and weakened. Where digital traces are lost, not only the likelihood of bringing the perpetrator to justice decreases, but also the very possibility of operational intervention in the movement of assets.

It should be emphasized that the problem of evidence is not a formal nit-picking of the system, but an objective condition for legal action. The state, no matter how great public compassion for the victim, cannot base restrictive measures only on assumption. The site is not entitled to block other people's assets without sufficient reason. A court cannot replace proof with empathy. That is why the delay in the first hours and days after the theft was discovered is so tragic. Every unsaved correspondence, every unmonitored address, every lost screenshot is not a trifle, but a potentially lost link in the chain of truth.

The fifth reason, which has no less public danger, is secondary fraud under the guise of assisting in the return of the stolen. Perhaps there is no more cynical form of exploitation of human misfortune than the deception of someone who has already been a victim once. Persons posing as lawyers, investigators, representatives of international organizations, employees of supervisory authorities, employees of stock exchanges, specialists in tracking transfers, private collectors, and financial monitoring experts begin to write or call the victim. They argue that the funds have already been found, that they can be "unfrozen," "withdrawn to a safe account," "legalize the return," "go through customs clearance," "pay a mandatory fee," "make a security payment," "open a transit account," "close the tax debt," "confirm the identity of the notary" or "activate the interstate transfer procedure."

Externally, such schemes are often built professionally: fake documents, pseudo-official forms, seals, imitation of business style, links to real institutions, demonstration of allegedly existing statements, fake interface images, false case numbers, fictitious certificates and even a staging of a multi-stage procedure that creates a sense of authenticity. But the internal mechanism remains the same: the victim again lures money, hiding behind the promise of their return. This is not a side, but a systemic layer of the criminal market. It feeds on despair, guilt, a thirst for justice and the very human inability to come to terms with loss. The offender knows: where a person has already lost a significant amount, he may be psychologically ready to give a little more, just not to admit the finality of the defeat and not give up hope.

From a scientific point of view, secondary fraud is especially dangerous because it relies not only on deception, but also on the traumatic state of the victim. After the first episode, a person's ability to soberly evaluate promises is impaired, suggestibility is increased, the desire for immediate correction of the situation is aggravated, criticality to the arguments of the "savior" is reduced. In such conditions, the promise of return acts almost like a painkiller: it does not convince logically, but captures emotionally. And therefore, the fight against this phenomenon requires not only criminal prosecution, but also extensive educational work. It is necessary to bluntly tell society: the requirement of advance payment for the promised return is one of the most characteristic signs of a new deception. Neither the "unblocking fee," nor the "advance payment to an international intermediary," nor the "insurance deposit," nor the "mandatory tax before payment" in themselves create a real mechanism for restoring the violated property right.

From what has been said follows a fundamental conclusion, which must be fixed clearly, strictly and without concessions to false consolation. Seeking legal protection is necessary, but the expectation of a guaranteed return of stolen funds in real practice is most often not justified. This formula may seem harsh, but scientific integrity requires just such a statement of the question. It is unacceptable to replace analysis with a compassionate illusion. The victim has the right to count on accepting the application, checking the circumstances, trying to trace the movement of assets, interacting with sites, collecting and evaluating evidence, and the state's criminal law response. But he should not become hostage to a false promise, as if the submission of the appeal itself triggers an almost guaranteed process of property recovery.

At the same time, such a harsh assessment does not mean that it is pointless to apply. On the contrary, without treatment, there is often not even a minimal chance of fixing the crime, documenting the circumstances and possible interference with the further movement of assets. The meaning of legal protection is not in the magical promise of the result, but in creating the maximum possible conditions for response. Yet the practical center of gravity must be shifted from subsequent "miraculous reparations" to warning, early threat recognition, immediate stopping of suspicious activities, and careful preservation of evidence. Here lies the crucial boundary between mature legal thinking and an infantile belief in automatically correcting any damage.

It is prevention that should be considered as the first line of protection of the property interests of citizens. Where the criminal scheme has not yet been completed, where the transfer has not yet been confirmed, where the suspicious requirement can still be checked, where access can still be closed, where correspondence can still be saved, where the site can still be notified, and the bank can be notified in a timely manner, the protection capabilities are many times higher than after the final scattering of traces. An early stop is almost always

more valuable than a subsequent pursuit. Preserving evidence is almost always more important than late explanations from memory. Discretion is almost always more reliable than hope. This is not a manifestation of pessimism, but a conclusion paid for by a huge array of real human losses.

Consequently, in scientific, legal and public discourse, it is necessary to abandon the dangerous romanticization of the procedure for returning stolen funds. It takes honest language that can call a spade a spade. If the funds passed through a chain of fragmented jurisdictions, were confirmed by the victims themselves under the influence of deception, quickly withdrawn through sites with limited readiness for immediate blocking, and evidence was lost or collected untimely, the likelihood of actual restoration of property status is objectively reduced. If, after that, the victim comes to the attention of "claimants" and "intermediaries" promising a refund for a preliminary fee, the risk of repeated loss becomes extremely high. The most dangerous lie in this space is the promise of a simple way out where it usually doesn't exist.

Therefore, a responsible professional position should be based on three pillars: legal protection is mandatory; there are usually no guarantees of return; prevention, prompt response and evidence-based discipline are crucial. This is the harsh but necessary truth. It is inconvenient, it deprives the soil of speculators of hope, it does not sell as easily as soothing promises - but it is this truth that serves to really protect a person. For where the illusion of guaranteed salvation ends, the only possible mature strategy begins: to warn, stop, fix and only then - to achieve everything achievable in the legal field, without replacing the struggle for justice with trade in hope.

Limited legal protection and institutional gaps

Victims in cases related to the theft of digital assets, indeed, often find themselves in a state of not only psychological confusion, but also actual legal isolation. This is not about the private experience of an individual, but about a systemic defect in the modern mechanism for protecting the right. When property is stolen from a person in an environment where money can be withdrawn in a matter of minutes, distributed to multiple addresses, converted into other digital accounting units, and then dissolved in a cross-border environment, he faces a special form of vulnerability. This vulnerability is born not only of the audacity of criminal trespass, but also of the disparity between the speed of harm and the slowness of the institutional response. It is in this gap that a dangerous space arises in which the offender acts with the expectation of a temporary advantage, and the victim - with the painful realization that every minute of delay reduces the likelihood of restoring the violated right.

The cross-border nature of digital assets radically changes the very architecture of crime and subsequent investigation. The crime no longer fits into traditional ideas about the territory, jurisdiction and locality of the trace. If, with a classic

property encroachment, it is possible to relatively quickly determine the place of the act, the direction of movement of funds, the circle of intermediaries and material media, then in the field of digital assets, the trace of a crime almost immediately acquires a distributed, multi-level and interstate character. Funds can be withdrawn through several sites of circulation of digital assets, then divided into many parts, then directed through mechanisms of concealment of origin, and then integrated into other calculated contours. At each stage, not only the form of accounting changes, but also the procedural complexity of access to information. As a result, law enforcement agencies of one state objectively face the limits of their own competence at the very moment when efficiency is crucial. Here, the structural contradiction is especially acute: the criminal operation is instantaneous and continuous, while interstate legal interaction still remains slow, formalized and dependent on multi-stage procedures.

The speed of moving funds in a digital environment is not just a technical feature, but an independent criminogenic factor. The criminal benefits from the fact that modern digital infrastructure allows for chains of operations with almost no time interval sufficient for external response. Minutes, and sometimes seconds, can pass from the moment of unauthorized seizure of access to the stage of multiple redistribution of assets. During this time, the victim is still only aware of the fact of the encroachment, trying to establish what exactly happened, collects confirming information, looks for site contacts, contacts the bank, prepares a statement. The state system is included in the process much later, when the assets have already been repeatedly moved, and their trace has lost its original transparency. Thus, time becomes not a neutral category, but a weapon of a criminal. And if the rule of law does not have mechanisms for immediate response, then it is actually forced to fight at a deliberately losing pace.

The complexity of the technical trace aggravates the situation of the victim and complicates the activities of the competent authorities. It is necessary to clearly understand: the digital footprint is not a simple sequence of records, available for direct perception and assessment. This is a set of information about the movement of assets, the actions of accounts, data about devices, time stamps, signs of network interaction, features of confirmation of operations, logic of routing means, the structure of connections between addresses and other information elements, the meaning of which is disclosed only with special training. It is here that one of the most disturbing features of the modern state of victim protection is revealed: legal recognition of the problem is not accompanied by sufficient technological readiness to disclose it. A statement can be accepted, but without immediate and qualified fixation of traces, it often loses a significant part of the evidence potential. Meanwhile, the digital environment is ruthless to delay: information can change, access is blocked, event logs are overwritten, and the connection between individual links of the criminal scheme is becoming less and less obvious.

The congestion of the law enforcement system in this area is becoming especially dangerous. The point is not only in the total volume of incoming reports of crimes, but also in the discrepancy between the complexity of the attacks under consideration and the resources allocated to their support. When one digital crime requires legal, technical, financial and interstate coordination at the same time, the traditional load-sharing model begins to fail. An employee who does not have enough time and specialized support is forced to act in conditions of lack of information, and each late decision may be irreparable. There is a danger of a formal approach: the application is accepted, materials are registered, individual requests are sent, but there is no holistic strategy for immediately suppressing the further movement of the stolen property. For the victim, this looks like a tacit admission of his own uselessness. For a criminal - as confirmation of calculations for impunity.

Deficits in specialized training represent perhaps one of the most significant drivers of institutional frailty. One cannot demand high efficiency from a system that is forced to respond to crimes of a new technological nature with old means of a conceptual and organizational nature. Without in-depth knowledge of the structure of digital registries, methods of concealing the movement of assets, the peculiarities of the operation of circulation sites, methods of establishing communication between addresses and specific persons, as well as without understanding the procedural value of various digital traces, the investigation inevitably loses the necessary acuity and accuracy. In such conditions, the victim often faces re-traumatization: he not only loses his property, but is also forced to explain the circumstances obvious to him to those bodies and organizations that themselves do not fully own the subject. This undermines confidence in justice as much as the criminal attack itself. Society is beginning to perceive the sphere of digital assets as a space in which law acts in a slow, uncertain and selective manner.

The systemic gap is especially pronounced in the interaction between the police, digital asset circulation sites and banking organizations. Each of these systems can indeed recognize the fact of disadvantage, but none individually is able to ensure the restoration of the violated property condition. The police have the right to accept the application, begin verification actions, request information, send instructions, initiate procedural decisions. However, without an established mechanism for accelerated international interaction, its capabilities remain limited by the national procedure, while the movement of digital assets has long gone beyond one jurisdiction. Contact sites can give a formal answer, request documents, confirm the presence of certain operations, and in some cases even temporarily restrict actions on specific accounts. But if the stolen assets have already gone further down the chain, if they are repeatedly redistributed, if a complex scheme of intermediate addresses and intermediaries is used, the site's capabilities become fragmented and belated. Banks, for their part, are able to fix the initial transfer, establish its details, and assess the circumstances of the

movement of funds at the initial stage. But as soon as property moves into the world of digital assets, their direct influence is sharply reduced. This is how a vicious zone of split responsibility is formed: each participant in the process sees only his own fragment of the picture, but the victim does not need a fragment, but the result.

It is from this fragmentation that a feeling of complete helplessness arises, which is so often reported by victims of digital fraud and other property attacks. The victim finds himself between several regulatory and organizational contours. In one, they require a strictly procedural statement of facts, in the other - technical evidence of account ownership, in the third - bank documents, in the fourth - evidence of the origin of funds, in the fifth - translated and certified materials for interstate circulation. The right, which by its nature should collect the scattered and connect the torn, in this area too often demonstrates the opposite: it splits the defense into many inconsistent procedural fragments. For the victim, this is not an abstract theory, but a harsh reality in which each instance seems to recognize the presence of trouble, but none assumes the obligation to overcome it entirely.

This situation has not only individual legal, but also pronounced socially dangerous consequences. Mass demoralization of victims is neither a metaphor nor an emotional exaggeration. This is a social effect that directly affects the level of latency of crime, confidence in the state and the overall stability of property turnover. When people come to the conclusion that it is pointless to seek protection, they stop reporting crimes, fixing traces in a timely manner, preserving evidence, initiating blocking measures and assisting the investigation. The offender, on the contrary, receives double benefits: he not only appropriates property, but also acts in an environment where the likelihood of institutional resistance is reduced due to public pessimism. Latency begins to feed crime, crime - distrust, and distrust - further latency. In this vicious circle, the very preventive function of law is destroyed. If the victim is convinced in advance that the system will not have time, will not understand or will not bring the case to the result, then the legal order loses part of its deterrent force even before the moment of a new encroachment.

That is why the task of public policy in this area should be formulated very clearly and uncompromisingly. It is not enough to limit ourselves to general calls for improving the digital literacy of the population or for improving legal regulation in an uncertain future. An architecture of immediate, specialized and legally related response is needed, in which the protection of the victim begins not after the completion of a long approval procedure, but at the time of the initial fixation of a criminal event. Such an architecture should include special rapid response mechanisms, unified protocols for fixing digital traces, accelerated channels of interaction between law enforcement agencies and digital asset circulation sites, as well as mandatory standards for verifying advertising placements that encourage citizens to participate in transactions with digital financial assets.

Creating specialized rapid response mechanisms is a top priority. In practical terms, this means the formation of such organizational and legal procedures that allow at an early stage to establish critical circumstances: the nature of unauthorized access, the addresses of the withdrawal of assets, the connection between the initial and subsequent operations, possible entry points into the regulated infrastructure, as well as persons and organizations that can immediately help to prevent further movement of property. The meaning of a quick response is not only to speed up work, but also to change the very logic of protection: from passive registration of already caused harm - to the active pursuit of stolen property in hot digital pursuit. This requires round-the-clock contact links, an understandable procedure for urgent transfer of information, templates for emergency notifications, criteria for the priority of processing appeals and a special regime of interdepartmental coordination for cases associated with the risk of instant withdrawal of assets.

No less important area is the development of standard protocols for fixing digital traces. Here, fragmentation and arbitrariness are unacceptable, since it is at an early stage that the evidentiary fate of the entire case is laid. The victim, duty officer, investigator, specialist, bank employee, site representative - all of them must act not by intuition, but according to uniform rules based on procedural reliability and technical sufficiency. The fixation protocol should cover not individual random information, but a complete picture of the initial digital footprint: information about accounts, addresses of receipt and disposal of assets, time stamps, notifications, device data, methods of confirming transactions, related correspondence, advertising materials through which the victim was involved in a criminal scheme, transfer details, as well as signs of subsequent redistribution of funds. The more detailed and accurate the original data set is recorded, the higher the probability of not only identifying the scheme, but also establishing repeated criminal practices in relation to an indefinite circle of persons.

Accelerated interaction between digital asset circulation sites and law enforcement agencies should exit the state of optional goodwill and acquire the properties of a mandatory legal standard. Today, too much depends on the internal rules of a particular site, on its place of registration, on the presence or absence of a clear procedure for responding to requests, on how quickly it is ready to provide information or limit operations on suspicious accounts. Such a situation is incompatible with the tasks of effective protection of victims, since the fate of the stolen property cannot depend on the unpredictability of private administrative practice. Regulatory response times, uniform requirements for the content of urgent requests, the procedure for confirming their receipt, the temporary retention of suspicious assets if there are sufficient grounds, as well as guarantees of subsequent judicial and procedural control, excluding arbitrariness, but not destroying efficiency, are required. In other words, we are

talking about the development of a balanced legal regime in which speed does not destroy legality, and legality does not paralyze speed.

The problem of advertising placements related to digital financial assets deserves special attention. Another painful zone opens here, where criminal activity is often disguised as outwardly conscientious information support. The victim often enters a dangerous scheme not through a deliberate search for illegal tools, but through publicly available materials stylized as investment recommendations, professional advice, analytical reviews or reports on supposedly legal income opportunities. Advertising in such cases becomes not a neutral channel for disseminating information, but part of a misleading mechanism. Consequently, public policy is obliged to establish standards for mandatory verification of advertising placements related to digital financial assets, including verification of the legal status of the advertiser, the reliability of statements about profitability, the availability of the necessary permits, the completeness of risk disclosure, as well as the authenticity of information about persons acting as organizers of the relevant proposals. If the space of public persuasion remains uncontrolled, the criminal scheme receives an invaluable advantage: it enters the consciousness of a citizen not as a threat, but as a promise.

It is necessary to emphasize the broader aspect: the protection of victims in the field of digital assets is not a peripheral area of criminal policy, but a test of the maturity of the modern rule of law. A state that is unable to provide an effective response to new forms of property encroachment risks losing confidence in one of the most sensitive areas - in the field of property protection. The right here must prove that it is able to follow the change in public relations not with fatal delay, but with proactive accuracy. This requires not only the adjustment of legislation, but also a deep institutional restructuring: training, the creation of specialized units, interdepartmental analytical coordination, the development of international treaty mechanisms, standardization of information exchange, equipping bodies with modern means of analyzing digital traces and the development of uniform methodological approaches for judicial and investigative practice.

Ultimately, the question is extremely acute. Either society will create a holistic system of operational and professional protection of victims in the field of digital assets, or it will continue to observe the expansion of the zone of legal helplessness, in which the offender acts faster than the state, more convincing than a warning, and more organized than protection. The most dangerous consequence here lies not only in property damage, but also in the gradual adaptation of society to the idea that in some sectors of the digital economy the right is doomed to delay in advance. This idea cannot be tolerated. It destroys respect for the law, corrupts the criminal with a sense of ease of profit and leaves the victim alone with a carefully organized system of alienation of his property. Therefore, the development of specialized rapid response mechanisms, standard

protocols for fixing digital traces, accelerated inter-institutional interaction and strict rules for checking advertising placements should not be considered as a desirable direction of development, but as an urgent requirement for legal and public safety.

Prevention: what should be the subject of public and scientific discussion

The main conclusion to which the analysis of modern criminal practice in the financial sector leads is as follows: the era of naive prevention has finally ended. Mere exhortations, general reminders of vigilance and formal "don't trust strangers" recommendations are no longer enough. They belonged to a time when criminal encroachment was built mainly on gross lies, direct deception and a relatively primitive imitation of legitimate activities. Today, society is dealing with a qualitatively different phenomenon. Modern fraud is not a random set of tricks, but an extensive system of psychological impact, organizational cover, information pressure and social camouflage. That is why opposition to it should also take on a systemic nature, covering not only the criminal prosecution of persons who have already committed a crime, but also the prevention of the very possibility of mass involvement of citizens in destructive schemes.

In this regard, it is fundamentally important to assert: prevention should become not an auxiliary, but a central line of public protection. This is not about one-time campaigns, not about short-term memos and not about on-duty publications after another high-profile incident, but about long-term, scientifically based and institutionally enshrined activities in which the state, the research community, the media, information dissemination sites, intermediaries in posting ads, educational institutions and professional associations participate. Each of these links performs a special task, and the loss of at least one element inevitably weakens the entire system. Where the state is limited to punishing the guilty, but does not create a coherent environment of prevention, crime gets space for endless reproduction. Where the scientific community does not explore the mechanisms of suggestion, mass trust and psychological vulnerability, prevention remains superficial. Where the media are chasing only an external sensation, without revealing the internal structure of the criminal scheme, society receives fear, but not knowledge. Where information dissemination sites and intermediaries in posting ads absolve themselves of all moral and legal responsibility, the offender receives not just a channel of access to the victim, but a halo of admissibility.

Therefore, we should talk about creating a unified preventive environment in which the prevention of fraud will not become a private initiative of individual departments, but a stable norm of public order. Such an environment involves the accumulation and constant updating of scientific information on methods of criminal influence, the development of uniform criteria for recognizing suspicious financial proposals, broad education of the population, conscientious regulation of public promotion of financial services, as well as the formation of

ethical and legal standards of conduct for all participants in the information appeal. Without this, society will repeatedly face the same tragic repetition: new names, new faces, new external forms - and at the same time the same internal mechanism of theft, based on credulity, anxiety, greedily cultivated hope and skillfully organized social pressure.

The question of what exactly should be the subject of mass education deserves special attention. For a long time, citizens were taught to recognize mainly external, technical signs of fake resources: erroneous designations in the network address, poor-quality page design, suspicious requests for information entry, lack of genuine registration data. All this remains important, but today it is decidedly not enough. Modern fraud isn't just about lying about money; this is primarily the engineering of trust, that is, the conscious construction of such a psychological environment in which a person gradually refuses a critical assessment of what is happening, begins to perceive the picture imposed on him as plausible and ultimately acts against his own interests, believing that he is acting reasonably.

That is why educational work should be turned not only to reason, but also to the emotional self-defense of the individual. Citizens need to be taught to recognize not only a fake document or a dubious page, but also the manipulative scenarios themselves, which precede theft and prepare the victim's consent. One of the most important such signals is artificial urgency. The criminal deprives a person of time to think, because he understands: free time is an ally of reason. When a potential victim is told that the decision must be made immediately, that the "window of opportunity" is about to close, that the funds must be transferred "now, otherwise it will be too late," we are not facing a sign of business dynamics, but a classic technique of suppressing critical thinking. The urgency in such schemes is not a requirement of circumstances, but an instrument of coercion. A person is torn from his usual rhythm of reasoning, placed in a time-deficient state and forced to submit to an imposed tempo at which doubt begins to be perceived as a dangerous delay.

An equally significant emotional marker is the cult of exclusivity. A potential victim is inspired by the idea that she opens a rare, inaccessible to most path to special well-being, a closed offer "for the elite," an opportunity to join the circle of those who know more than others. In this technique, deep psychological work is hidden: a person is offered not just income, but a symbolic elevation over others, participation in the imaginary elite, a sense of dedication to a secret that is supposedly hidden from "ordinary" people. The victim is bought not only by the promise of benefits, but also by flattery. She is not offered a financial solution, but a new identity - the image of a person knowledgeable, bold, ahead of others. It is here that criminal influence connects the economic motive with social vanity, turning deception into a form of self-exertion.

Among the most dangerous signs is the promise of too high, and more importantly, too even profitability. In normal business, profits are always

associated with risk, variability, unfavorable periods, the influence of many circumstances. Where the public is promised almost mechanical multiplication of funds, which does not depend on market fluctuations, or on the state of production, or on political events, or on ordinary economic uncertainty, one should see not a miracle of efficiency, but an attempt to replace economic reality with a myth of guaranteed enrichment. Especially alarming is not only the height of the declared indicators, but also their smoothness, monotony, ostentatious stability. The criminal scheme likes to draw income as something continuous, almost natural, as if it knows neither recessions, nor mistakes, nor losses. But it is precisely such deliberate correctness that should cause the most distrust in a prepared person. In a genuine economy, there are no perfectly straight lines; they arise mainly where, instead of economic reality, there is a carefully composed legend.

A very characteristic element of modern schemes is the so-called multi-layered pseudo-command - an artificially created impression that there is an extensive team of specialists behind the proposal, each of which is responsible for a separate area of work. "Analysts," "accompanying specialists," "senior curators," "financial advisers," "technical employees" can be consistently presented to a potential victim, and all this fictional hierarchy is needed for one purpose: to create a feeling of institutional solidity. A single liar is less credible than an institution's organized appearance. When a person encounters not one interlocutor, but with a whole chain of persons using agreed vocabulary, uniform scenarios of persuasion and mutual confirmation of what has been said, he develops a false impression of legality, professionalism and scale. Meanwhile, before him is often not a team of specialists, but a production, where the roles are distributed for the purpose of psychological pressure. Therefore, the population needs to be specially trained in the recognition of such theatrical structures, explaining that the abundance of "posts" and "escort levels" in itself does not prove the reality of the organization, but, on the contrary, can serve as a disguise technique.

An extremely important sign of criminal influence is the requirement of secrecy. When a person is told that a proposal cannot be told to relatives, friends, colleagues, lawyers, bank employees or other persons capable of giving a sober assessment, this should be considered one of the most alarming signals. Secrecy in such cases is needed not to protect the interests of the client, but to isolate the victim from a possible saving objection. The criminal seeks to narrow the circle of communication of a person to a controlled channel in which there will be no alternative interpretation of what is happening. In essence, we are talking about the preliminary destruction of public relations as a condition for future theft. The fewer independent voices around the victim, the easier it is for the criminal group to consolidate its own version of reality. That is why it is necessary to persistently repeat in educational materials: the requirement of silence about a financial proposal is not a sign of privilege, it is a sign of danger.

The depreciation of the opinion of loved ones is associated with the same mechanism. Criminal schemes often form in advance in the victim distrust of those who could stop her. Relatives and friends are presented as people who are "backward," "do not understand anything in modern ways of earning money," "think too narrowly," "fear of success," "envy the brave." Such rhetoric performs a destructive function: it neutralizes the natural family and friendly defense in advance. A person is torn not only from money, but also from his environment of mutual support. In this sense, modern fraud is dangerous not only by property loss; it invades the very fabric of trusting relationships, undermines family unity, sows suspicion, makes you perceive care as an obstacle. Therefore, the fight against such schemes should include the restoration of public respect for the collective verification of dubious decisions. A simple but fundamental idea should be affirmed: in matters of transferring significant funds, advice with loved ones is not a weakness, but a sign of mature responsibility.

No less alarming is the transfer of communication from the public environment to closed personal channels. At the first stage, the offender can use a relatively open space, but then almost inevitably seeks to transfer the interaction to where there is no external control, where it is impossible to easily check the content of promises, where it is more difficult to complain, record the course of influence and warn others. Closeness is a natural environment of criminal manipulation. It is more convenient to correct the legend in it, increase pressure, dose information, remove traces, change the key from friendly to threatening and vice versa, without fear of public exposure. Therefore, the population should be taught to perceive such a translation of communication not as a natural continuation of "individual accompaniment," but as a risky stage, after which the likelihood of abuse increases sharply. The less publicity and verifiability a deal has, the more likely it is to be an instrument of theft.

Finally, it is necessary to explain in particular detail to citizens the mechanism of constant alternation of hope and anxiety - one of the most effective ways of psychological submission. A person is promised close success, then they report a sudden obstacle; either they draw rapid enrichment, then they scare them with the threat of losing already invested funds; then soothed, then reintroduced into a state of acute tension. This pendulum effect is not accidental. It depletes the will, deprives a person of a stable position, makes him dependent on the next message of the criminal as the only source of relief. The victim is held not by the logic of benefit, but by the rhythm of emotional training. Hope does not allow us to retreat, anxiety does not allow us to stop, and in this painful change of states, a person often transfers new amounts, guided no longer by calculation, but by the desire to regain a sense of inner stability at any cost. For scientifically based prevention, it is extremely important to directly name this mechanism and include its description in educational, educational and legal materials. As long as society sees in fraud only a false promise of money, it does not understand the depth of psychological abuse to which the victim is subjected.

All this leads to the following fundamental conclusion: education should educate not only technical awareness, but also psychological literacy. A person must be able to recognize the moment when he is influenced through fear of missing an opportunity, through vanity, through loneliness, through a thirst for a quick resolution of anxiety, through the substitution of reasoning with suggestion. In other words, the citizen needs to convey not a list of private tricks, which will always be incomplete, but an understanding of the general laws of criminal pressure. Only such knowledge has genuine stability: schemes change names, design and vocabulary, but their psychological framework is surprisingly constant.

A separate and especially heated discussion requires the question of the responsibility of those who post and disseminate information about dubious financial services to a wide audience. Here, public thought has been content for too long with the convenient formula that the answer is only the direct offender, while the rest of the chain allegedly remain neutral intermediaries. However, this position is less and less resistant to moral and legal criticism. Anyone who provides a criminal scheme with a channel of public suggestion cannot endlessly hide behind the mask of an indifferent technical function. Public fame, social authority, high attendance of the information platform, the reputational weight of the advertising distributor - all this has an independent power of persuasion. For many citizens, the very fact of the appearance of a proposal in a known space is already perceived as an indirect confirmation of its admissibility. Consequently, when a dubious financial service is widely disseminated through channels that enjoy public trust, the offender actually borrows someone else's reputation. He steals not only the money of future victims, but also the symbolic capital of public recognition.

That is why it is unacceptable that a sign of public fame turns into an instrument of someone else's theft without any consequences for the distributor of information. Of course, the issue should not be resolved primitively and without distinguishing between degrees of guilt. But it is equally obvious that the complete removal of responsibility from the infrastructure of legitimation means the actual encouragement of indifference. If a person, organization or site systematically benefits from the placement of suspicious financial proposals without taking reasonable verification measures, without responding to signs of fraud, without creating effective pre-selection procedures and subsequent cessation of the distribution of hazardous materials, then this is no longer a random technical error, but socially harmful connivance. The legal order, seriously aimed at protecting citizens, is obliged to discuss and develop mechanisms of proportionate responsibility for such connivance.

In scientific and legal terms, it is especially important to separate several levels of participation. One level is the direct perpetrator of the theft, organizing a false scheme, conducting correspondence, accepting funds and hiding with the stolen.

Another level is the persons and structures that create the appearance of authenticity for this scheme: they post ads, provide mass promotion, accompany public presence, allow the use of their own reputation resources without due diligence. Without the second level, the first would often lose the breadth of coverage that turns a single deception into a mass disaster. Therefore, talking about the responsibility of legitimation infrastructure is not an attempt to blur the guilt of a direct criminal; on the contrary, it is the desire to see the criminal phenomenon in its full social scope. Society loses whenever it treats embezzlement too narrowly - like a victim meeting with an individual malevolent person - and overlooks the kind of mediation system that made that meeting likely and compelling.

Here it is necessary to say about the moral dimension of the problem. Whenever a distribution site, ad intermediary or public figure benefits from promoting a dubious financial product without asking themselves the consequences for many gullible people, there is a dangerous normalization of public cynicism. The profit received at the cost of someone else's ruin does not become less shameful because it is formalized by a contract for the dissemination of information. On the contrary, the more respectable the outer shell of such participation looks, the deeper the undermining of public morality. People are beginning to see that there is no insurmountable line between crime and a law-abiding environment, that theft can rely on quite ordinary mechanisms of fame, reach and commercial interest. This destroys confidence not only in financial treatment, but also in public institutions themselves.

Hence the requirement to develop stricter rules of good faith for all entities involved in the public promotion of financial proposals. Such rules should include the obligation to pre-check the status of the advertised service, clear criteria for identifying signs of unfair promotion, the obligation to immediately stop the dissemination of information upon receipt of reasonable signals about the fraudulent nature of the offer, as well as the establishment of proportionate legal consequences in cases of systematic disregard of obvious risks. But something else is even more important and deeper: society must abandon the illusion that the neutral shell of the dissemination of information does not affect the trust of citizens. Influence exists, it is great, and that is why it should be associated with responsibility.

Thus, if society really intends to protect citizens in the face of rapidly increasing fraudulent practices, it is obliged to rethink the very philosophy of counteraction. It is not enough to wait for the theft to occur to then search for the culprit. Nor is it enough to limit ourselves to an edifying formula about personal discretion. A transition is needed from moralizing to a system, from random response to sustained warning, from a narrow understanding of deception to a holistic analysis of mechanisms of trust, suggestion and legitimation. Only with this approach is a real reduction in public vulnerability possible.

The final thesis should be formulated very clearly. Modern fraud wins where society continues to regard it as a private story of someone else's credulity; it retreats only where the state and public institutions recognize it as a complex technology for seizing trust and build an equally complex defense system. Therefore, the task of our time is not only to expose individual criminals, but also to deprive the crime of its breeding ground: ignorant hope, irresponsible publicity, commercial indifference, institutional disunity and the habit of considering someone else's misfortune as a result of personal weakness alone. Until this is done, each new warning will be belated. But if such systemic work becomes a reality, society will have a chance not only to reduce the number of victims, but also to restore what criminal schemes destroy in the first place - trust as the basis of civil life.

Conclusion

Modern fraud in the field of digital financial assets should be considered not as a set of disparate episodes of property deception, not as an accidental heap of private criminal practices and not as a by-product of a rapidly developing economic environment, but as an existing system of multi-level criminal influence, in which social engineering, psychological pressure, technical imitation of authenticity, media mediation, fake publicity and calculated use of insufficient certainty of legal regulation. Its public danger is fundamentally wider than causing direct property damage to an individual victim. In fact, we are talking about the defeat of the very foundations of public trust: trust in information, trust in institutions, trust in professional expertise, trust in the promise of legality as such. Where a person loses the ability to distinguish between genuine and staged, verified and fake, reasonable and imposed, there is not just an economic risk, but a space of deep anthropological vulnerability, in which the object of encroachment is no longer an account or an electronic wallet, but personal autonomy, the ability to independent judgment, dignity and will.

This is the qualitative difference between the latest fraudulent schemes and traditional forms of deception. Previously, a criminal action was often built around a one-time episode - a false promise, direct substitution, gross falsification, the rapid disappearance of a criminal after receiving money. Now we have an extensive criminal architecture, based on the long-term support of the victim, on the consistent building of trusting relationships, on modeling the victim's feeling of personal involvement in the supposedly rational and controlled process of generating income. This fraud has long since ceased to be the craft of the occasional adventurer; it has become a disciplined practice of systematically influencing a person's perception, emotions, and behavior. Its performers study the victim's reaction, dose incentives, select arguments, alternate reassurance and alarming pressure, create the illusion of expert guardianship, involve "successful participants" in artificially constructed communities, demonstrate fake evidence of profitability and play out entire

scenes of external legitimacy. Thus, the crime is transferred from the plane of one-time theft to the plane of phased submission of will.

The most dangerous schemes are indeed based on the slow and methodical erosion of the victim's critical ability. At first, a person is offered not risk, but hope, not an adventure, but the appearance of a reasonable opportunity, not a gross violation of common sense, but a carefully directed picture of successful participation in a new financial reality. Then comes the first reinforcement: a little "success," an imaginary accrual of profits, a demonstration of a growing balance, prompt responses from the "curator," friendly support from imaginary community participants. After that, the next stage is included - linking the victim to the actions already performed. A person begins to defend the decision, because admitting a mistake means not only the likely loss of funds, but also a painful blow to self-esteem. It is here that fraudsters introduce new grounds for investment: the need to increase the amount for the sake of access to a "more favorable level," the urgent need to close the "technical gap," pay the "commission," "insurance deposit," "check the purity of funds," "tax payment" or other fictitious condition for withdrawing money. When the victim has a doubt, he is offered not a retreat, but another chance for salvation, and thus the deception takes the form of a psychological funnel, where each previous step is used as an argument in favor of the next. This is one of the most cynical features of modern digital fraud: the victim is brought to a self-destructive decision not through open coercion, but through the staging of free, reasonable and supposedly informed choices.

Fake stock pages, fictitious personal yield cabinets, imaginary price difference schemes between sites, stories about safe passive remuneration, staged reviews, pseudo-news publications, fake consultants, false IDs, respectable meeting rooms, staged conference photos, international license announcements and ostentatious media openness are not a chaotic set of tricks, but elements of a single criminal system for legitimizing deception Each of these details works to create a special effect - the effect of normality, within which the obviously abnormal begins to be perceived as familiar, and the incredible - as acceptable. A fake personal account is needed not only for visual deception, but also for emotional consolidation of income expectations; a false scheme of price differences between sites - not only for a pseudo-economic explanation of profits, but also to inspire a sense of intellectual advantage over "ordinary" market participants; imaginary professional terminology - not only to decorate the speech of the criminal, but also to suppress resistance from the victim through linguistic asymmetry. A person, faced with a large number of outwardly agreed signs of legality, often begins to consider his own alertness as a manifestation of ignorance, and doubt as a sign of personal incompetence. So the crime reaches the highest degree of cunning: it forces the victim to interpret common sense as an obstacle to success.

A special role in the reproduction of these schemes was taken by messenger sites, primarily Telegram, where the combination of high speed of dissemination of information, relative anonymity, ease of creating numerous channels and communities, the possibility of direct access to the user and limited external verification created an extremely favorable environment for criminal networks. Here pseudo-communities of trust are formed, in which each element of communication works on the effect of mass confirmation. Closed groups create the illusion of chosenness; many messages of the same type - the illusion of consensus; quickly deleted publications - a sense of efficiency and exclusivity; a network of interconnected accounts - the impression of a living human environment. In such an environment, the victim is not in front of a single attacker, but inside an artificially constructed social world, where not only information is forged, but also the very fabric of interpersonal communication. This is a special danger of messenger mediation: the crime disguises itself as a community, the exploitation of trust as a friendly council, the imposed investment model as an exchange of experience, and recruitment as a voluntary adherence to successful practice.

Therefore, the public reaction to this phenomenon cannot be limited to either moral panic or superficial accusations against the victims themselves, as if the victim was invariably guilty of his own gullibility. Such a position is not only scientifically untenable, but also socially destructive. It closes the way to an adequate understanding of the mechanisms of crime, interferes with the timely appeal for help, enhances the shame of the victim and, therefore, objectively works in the interests of the criminal environment. It is necessary to conduct not hysterical, but extremely sober, evidence-based and uncompromising conversation about the structural conditions for the spread of digital fraud. Such a conversation should include an analysis of the advertising infrastructure through which pseudo-financial proposals are promoted; a study of language and visual techniques for imitating legality; studying personal impact algorithms; assessment of the role of intermediaries providing mass reach channels; as well as the development of transparent and mandatory standards for verifying information about financial products distributed in the digital environment. In other words, society is obliged to stop seeing in each episode only a private tragedy and begin to recognize in these episodes the manifestation of a single criminal order.

No less important is the legal conclusion that follows from the accumulated array of empirical observations: the illusion of easy recoverability of stolen funds is one of the most dangerous misconceptions associated with digital fraud. In practice, returns are often extremely difficult due to multi-stage movement of funds, the use of cross-border channels, substitution of traces, splitting of amounts, the involvement of formally uninvolved persons and the rapid disappearance of digital traces. Even where individual elements of the movement of funds can be fixed, this does not guarantee either the establishment of the final beneficiary, or

a quick procedural response, or the actual restoration of the property status of the victim. Moreover, at the stage after theft, a secondary wave of criminal influence often arises: the victim is offered "help in returning," luring out new payments under the pretext of legal support, a special investigation, accelerated unlocking or a mandatory pre-payment. Thus, the post-criminal stage itself becomes a continuation of the initial deception. Hence the fundamental practical conclusion follows: the main line of defense does not pass where the subsequent miraculous salvation is promised, but where early recognition of the scheme, immediate termination of communication, fixation of all available evidence, preservation of correspondence, payment information, transfer addresses, screen shots, as well as psychological support for the victim, necessary to prevent further mistakes made in a state of panic, shame and despair.

Therefore, prevention in this area should be understood significantly wider than the usual informing of the population about "suspicious promises of high profitability." It is necessary to form a culture of evidence-based alertness, in which any proposal related to investing in digital assets is assessed not by the strength of the emotional impression, but by the totality of verified signs: legal certainty of a person, the presence of a verifiable business history, transparency of the income generation model, the possibility of independent verification of the declared transactions, the absence of pressure on the urgency of the decision, the absence of requirements for additional payments for the sake of withdrawal of funds, as well as the absence of closed communication circuits in which all information is controlled exclusively by the initiator of the transaction. It is necessary to foster not fear of new technologies as such, but the intellectual discipline of handling them. We are talking about the skill to recognize manipulative speech, about the ability to notice an artificially created time deficit, about the habit of checking information on independent sources, about the willingness to suspend actions when at least one significant discrepancy occurs. It is this kind of discipline, not the rhetoric of easy money, that is a genuine sign of a mature attitude towards the digital economy.

At the same time, it would be a mistake to reduce the problem only to individual caution. No single user is able to single-handedly compensate for all the systemic flaws in an environment in which criminals enjoy high communication speed, distraction, technological complexity and legal fragmentation. Therefore, the collective willingness of society to call what is happening by their proper names is necessary: not an "unsuccessful investment" when there was an organized misrepresentation; not "controversial entrepreneurial practice" when it comes to deliberately staging fictitious returns; not "aggressive promotion of services," when targeted psychological subordination of the victim is carried out. The language of description here is not secondary, but fundamental. Where crime is mitigated by euphemisms, the threshold for public response is lowered; where manipulation is called "marketing device" and embezzlement is called "user risk," the criminal model gains additional protection in the form of speech

normalization. The scientific and legal description should be accurate, merciless to the substitution of concepts and free from rhetoric justifying actual violence against trust.

Ultimately, we are not just a new type of property encroachment caused by the technical development of economic turnover. Before us is a large-scale attack on the foundations of human autonomy, disguised as the language of progress, profit, freedom of choice and financial self-determination. That is why the analysis of digital fraud in the field of financial assets should be conducted at the intersection of criminology, psychology, sociology of trust, communication theory and legal science. Only such interdisciplinary consideration allows us to see in individual episodes not a random chain of disasters, but a reproducible model of submission based on the exploitation of hope, fear, cognitive overload, shame and social isolation. The longer society perceives such embezzlement as the sum of private misfortunes, the stronger the criminal industry itself will become, the more perfect - its means of disguise, the deeper - the erosion of trust, without which neither economic exchange, nor legal stability, nor normal public life are possible.

Hence the main result of this study: the fight against fraud in the field of digital financial assets requires not only improving law enforcement practice, but also moral, intellectual and institutional mobilization of society. It is necessary to protect not only money, but also the ability of a person not to become the object of controlled suggestion; not only property interests, but also the dignity of the individual; not only the security of settlements, but also the very possibility of existence in an environment where trust does not turn into raw materials for theft. If this task is not realized in all its depth, criminal networks will continue to expand their influence, hiding behind the language of novelty and the promise of easy well-being. If society develops a clear conceptual framework, strengthens early warning mechanisms, refuses to accuse the victim and requires real responsibility from all links of the digital intermediary environment, then it will be possible not just to respond to individual episodes, but to consistently limit the very social soil on which this crime grows. Therefore, the key conclusion is that modern digital fraud is not a peripheral anomaly of financial development, but one of the central threats to public trust, legal stability and human independence, and therefore countering it should not be a matter of private precaution, but of a national legal and cultural strategy.