VIKING NET

DEFENSE · DIGITAL FORENSICS

DIGITAL FORENSICS & FRAUD INVESTIGATION REPORT

Fraudulent Crypto Investment Platform

Subject: **dkmrf.com** / brand **"Crypto Market"**

Booking.com task-scam to pig-butchering deposit fraud

CASE NUMBER
VN-2026-0001

REPORT DATE
June 3, 2026 (Public Sample)

PREPARED FOR
[Client name withheld]

PREPARED BY
Viking Net Defense, OSINT Unit

INVESTIGATION TYPE
Open-source intelligence (OSINT)

STATUS
Active scam, victim currently targeted

SAMPLE · REDACTED

Public sample. This is a redacted demonstration of a Viking Net Defense forensic report. Client identifiers, the impersonated firm name, and sensitive indicators have been removed, and the evidence exhibits are withheld. The full report delivered to a client contains complete details and chain-of-custody.

DOCUMENT CONTROL

FIELD	DETAIL
Case number	VN-2026-0001 (Revision 2: expanded with a second batch of victim evidence)
Subject	Fraudulent crypto platform dkmrf.com, brand "Crypto Market"
Classification	**Confidential.** Share only with the victim, their counsel, and law-enforcement.
Prepared by	Viking Net Defense, a service of Viking Net LLC, San Antonio, Texas · vikingnetdefense.com · info@vikingnetllc.com
Method	Passive open-source intelligence only. No system was accessed, attacked, or logged into. No law was broken producing this report.
Evidence basis	Live technical reconnaissance (2026-06-03) plus fourteen screenshots supplied by the victim (Exhibits A to N).
Confidence model	VERIFIED confirmed this engagement INFERRED strong pattern, not literally proven UNKNOWN not obtainable by OSINT

1. WHAT HAPPENED, IN PLAIN ENGLISH

A stranger offered the client an easy online "job": tap a few buttons on booking.com a handful of times a day for small payments. After he was paid a little and trusted it, he was moved to a slick crypto website (dkmrf.com) and told that to earn more he had to "complete trader tasks," which meant **sending in his own money**. The website showed his balance going up and big profits coming. None of it is real. The site is a fake controlled entirely by the scammers, the "profits" are just numbers they type on a screen, and the money he sent is already gone to them.

They are now doing the final stage: telling him he must pay more (a fake "insurance contract," fake "taxes," and a fake "payout password") before he can withdraw. **He never will.** Every extra payment only feeds the scam. This report lays out exactly what we found, who the players are, where the trail leads, where it goes cold, and precisely what the client should do today.

2. EXECUTIVE SUMMARY

dkmrf.com is a fraudulent crypto platform, not a real exchange. It is the end of a "task scam to pig-butchering" pipeline run through a large Telegram group. Deposits are taken in Bitcoin and a fabricated balance is shown to simulate profit. The operation is in its extraction phase, using a forged insurance contract, escalating "trader task" deposit demands of **2,560 to 4,820 EUR**, and a fake "payout password" to pull out as much money as possible.

Time-critical. The scheme is active right now (documents dated 03.06.2026, handlers last seen live, a call in progress during a screenshot). The one funded payment we can see, **189 EUR, went via PayPal to a private individual**. PayPal and the funding bank are live clawback levers only if acted on immediately. See Section 12.

The findings that move this from "likely a scam" to a documented, multi-layer fraud:

1. The platform is **disposable and anonymous** (registered 2026-03-29, one-year term, hidden behind privacy protection and Cloudflare) and fakes a live "market" using a **free public Binance price feed.** VERIFIED
2. The "trading" screen is a **rigged fixed-time / binary-options game** ("up or down in 180 seconds"), a product that is **banned for retail investors in Germany and the EU**. The house sets every outcome. VERIFIED
3. The forged insurance contract uses the **stolen identity of a real FCA-regulated UK firm** (the impersonated UK firm) that publicly states it does not touch crypto, plus a non-existent "Ministry of Finance and Statistics." VERIFIED
4. The recruiter identity "**Josie Bruns**" is a documented, reused task-scam alias. VERIFIED
5. Even the platform's **graphics betray the fraud**: off-center buttons, broken machine-translated menus, a leftover Croatian word, and inconsistent capitalization (Section 8.8). VERIFIED

3. SCOPE, AUTHORIZATION & METHOD

Authorization. Conducted at the request of a referring party on behalf of the victim. Defensive, victim-assistance investigation.

Method. Passive OSINT only: public DNS / WHOIS, TLS certificate transparency, IP and routing data, the platform's own publicly served web code, public corporate (Companies House) and regulatory (FCA, BaFin, ESMA) sources, public scam and reputation databases, and analysis of fourteen victim screenshots. A coordinated set of specialist research agents ran the reputation, scam-pattern, fake-exchange, document, corporate-regulatory, persona, money-rail, and new-indicator tracks in parallel. **No login, intrusion, or contact with the offenders.**

4. INDICATORS OF COMPROMISE (IOCS)

TYPE	INDICATOR	NOTE	CONF.
Domain	`dkmrf.com`	Fake "Crypto Market" platform. Created 2026-03-29, 1-yr reg, Amazon Registrar, Cloudflare DNS, no MX/TXT.	V
Domain (sibling)	`dkmry.com`	Near-twin already flagged as a crypto scam. Indicates a rotating "dkm**" cluster.	V
IPv4	`104.21.91.76, 172.67.212.14`	Cloudflare proxy (AS13335); hides true origin.	V
Price feed	`data-api.binance.vision`	Free public Binance feed. The platform's only "connection to the crypto world."	V
Telegram channel	`t.me/[REDACTED]`	Private "task" channel invite. Perishable, capture fast. No public report found.	V
Recruiter	"Josie Bruns" `@Josie6077`	Documented reused task-scam recruiter alias.	V
Handler	"Michael" `@M19951103`	"Investment manager / mentor." Ran trades, sent contract, issued payout password.	V
Victim (their system)	"[client]" / `[client email redacted]`	Victim's display name and "employee code" inside the scam.	V
Money mule	"[money mule, name redacted]"	PayPal recipient of 189 EUR. Private individual, not a company.	V
Fake payout token	`[REDACTED]`	"Auszahlungspasswort" given to unlock withdrawal. Functionless prop.	V
Impersonated firm	a real, FCA-regulated UK wealth firm (name withheld)	Real FCA firm, Companies House [reg. no. withheld]. Name stolen for the seal.	V
Fake authorities	"Ministry of Finance and Statistics"; "Finanzdirektor"	Invented oversight/figures to sound official.	V
Toolkit leaks	`"Platiti" (Croatian);  (Chinese)`	Leftover strings from a multi-language white-label scam kit.	V
Deposit demands	`2,560 / 3,520 / 4,820 EUR`	"Trader task" walls (Daten 1/2/3) at 30/35/40%, fake "refunds" 3,328 / 4,752 / 6,748 EUR.	V

5. EVIDENCE INVENTORY & CHAIN OF CUSTODY

EX.	DESCRIPTION	SHA-256 (FIRST 16)
A	Forged "Versicherungsvertrag" (insurance contract), the impersonated UK firm seal, sent by "Michael"	`46df93b882ca776b`
B	Recruiter "Josie Bruns" @Josie6077 profile; booking.com task + PayPal-to-mule + commission tiers	`022ddb8aa2417419`
C	Handler "Michael" @M19951103 profile; fake trading dashboard	`5715dc8c1e3f640a`
D	"Trader task" deposit table (Daten 1/2/3: 2,560 / 3,520 / 4,820 EUR)	`a4ef4bf6386db4b9`
E	"Order complete, no further orders" system dialog	`4ea6e0ad9a8db12f`
F	Rigged binary-options app (BTC/USDT, Long/Short, 180s/120s/60s = 30/35/40%)	`987f08913d1e9c32`
G	"Aufgabenzeit" 18-task daily schedule infographic	`c805843e511dd097`
H	"Questbelohnungen" reward-ladder infographic (claims 389 EUR/day)	`7fc03137adbafd4d`
I	Telegram: dashboard + Josie "win-win-win" trader-task explanation	`2aaa0fde84915cf1`
J	Telegram: task rules + channel invite link	`c0010d95ac529e9d`
K	Telegram: task rules (continued)	`8131fb30ac0421df`
L	Telegram: Michael directs to dkmrf.com + system rules	`b034ed04b2719b91`
M	Telegram: Michael's full "system rules" (prepayment, no-compensation, Finanzdirektor)	`b317cb3320bd699d`
N	Telegram: 6-step trade script + payout-password gate ([REDACTED])	`d0fbbeeb10bcc311`

Exhibits preserved at full resolution in the case folder; SHA-256 recorded at intake. Selected exhibits reproduced in Appendix D.

6. FINDINGS

6.1 Domain & hosting infrastructure

In plain terms: this "company" did not exist ten weeks ago, hides who owns it, and rented its name for only a year. Real financial firms do not do this.

CREATED	**2026-03-29** (about 10 weeks old). Registered through 2027-03-29 only.
REGISTRAR / DNS	Amazon Registrar; Cloudflare nameservers and proxy (hides the true origin server).
OWNER	Hidden behind a privacy proxy. No identifiable person or company. No MX/TXT records (no real mail or domain verification).
WEB APP	Empty-shell single-page app: blank page title, generic framework bundle, no company name or legal imprint.

6.2 It is a fake exchange (the "does it even take hardware?" question)

A real exchange needs a matching engine and order book, deep liquidity, real custody (hot/cold wallets, HSMs, multisig), banking rails, KYC/AML, licensing (FinCEN and state licenses in the US; MiCA and BaFin in the EU), 24/7 security, and audited reserves: tens of millions of dollars and hundreds of people. **dkmrf.com has none of it.** Its own code calls a **free public Binance price feed**; showing hundreds of live coin prices is one free API call, a price ticker, not an exchange. Balances, trades, and profits are numbers in a database the operator edits at will; deposits land in the operator's wallet on arrival.

In plain terms: the flashy price screen is the cheapest part to fake. It proves nothing.

6.3 The "trading" is a rigged binary-options game (illegal product)

The trade screen (Exhibit F) offers "BTC/USDT", "Long Kaufen / Short Kaufen", and fixed timers **180s / 120s / 60s mapped to fixed payouts 30% / 35% / 40%**, with an amount field and an "estimated earnings" line. This is a **fixed-time / binary-options ("guess up or down") interface**, not real trading. The operator is the counterparty and sets every outcome (regulators document platforms that extend the timer until a winning trade becomes a loss). Critically, retail binary options are **banned in the EU (ESMA, 2018) and permanently in Germany (BaFin, 2019)**, so the product is illegal before any fraud is added. "Michael" even scripts it (Exhibit N): open dkmrf.com, BTC/USDT, Long, 180 seconds, amount 33, submit, screenshot, reply "OK."

6.4 The fake "job": a gamified task system

The scam is dressed as a structured job (Exhibits G, H, J, K). **18 tasks per day, 09:00 to 20:30, a new one every 30 minutes, 2 EUR each.** Positions **4, 8, 12, 16 are "Händler-Aufgaben" (trader tasks)**: these are the deposit traps; the rest are harmless booking.com "tasks." A reward ladder (complete 4 to earn 6 EUR, 8 to earn 15, 12 to earn 80, 18 to earn 180, claimed 389 EUR/day total) and a coercion rule (miss a trader task and tomorrow's pay drops to 0.5 EUR) keep the victim engaged and afraid to stop. Pay is "released at 8 EUR to your bank account," which is the hook that first makes it feel real.

In plain terms: the "job," the levels, the daily wage, the bonuses, all of it is a game designed to make depositing feel like work you are owed for.

6.5 The personas and the victim

"Josie Bruns" (@Josie6077), recruiter: young-woman photo (likely AI or stolen), Telegram Premium badge (purchasable, not verification). The name is documented across anti-fraud reports as a reused task-scam recruiter alias. **"Michael" (@M19951103)**, "investment manager / mentor": ran the dashboard, sent the contract, issued the payout password, last seen live. The victim appears in their system as **"[client]" ([client email redacted])**.

6.6 The money trail and escalating deposit demands

The one funded payment visible is **189 EUR via PayPal to a private individual, "[money mule, name redacted]"** (German PayPal person-to-person wording), the signature of a money mule. If sent "Friends & Family" (likely, confirm in PayPal Activity), there is essentially no buyer protection. The fabricated dashboard showed balances of 76 to 935 EUR at different times (numbers the operator changes at will). The extraction ask is far larger (Exhibit D):

"TASK"	DEMANDED DEPOSIT	RATE	"COMMISSION"	PROMISED "REFUND"
Daten 1	2,560 EUR	30%	768 EUR	3,328 EUR
Daten 2	3,520 EUR	35%	1,232 EUR	4,752 EUR
Daten 3	4,820 EUR	40%	1,928 EUR	6,748 EUR

Each "trader task" demands a larger deposit and promises a refund that exceeds it. The refund never comes; the wall just rises. **PayPal holds the real identity behind "[money mule, name redacted],"** which is why the PayPal fraud report (Section 12) is the single highest-value recovery action.

6.7 The documents (the paperwork is the weapon)

Three layers of fake paperwork manufacture pressure: (1) the **insurance contract** (Exhibit A, full translation in Appendix A) that forbids withdrawals, sets a "profit must exceed 30%" lock, cites a fake ministry, and says they may withhold the "payout code"; (2) **Michael's "system rules"** (Exhibit M) forbidding private investment, warning of "no compensation," and pointing to a "Finanzdirektor" to "activate the payout channel"; and (3) the **"Auszahlungspasswort" [REDACTED]** (Exhibit N), a prop code handed over by a fake "reception" to "unlock" a withdrawal that never happens. German lawyers warn that signing such PDFs has been used to open loans in victims' names. **The victim should not sign or pay anything.**

6.8 Regulatory impersonation

The contract's seal names **"a real, FCA-regulated UK wealth firm (name withheld), United Kingdom,"** a real, active, FCA-regulated wealth firm (Companies House [reg. no. withheld], incorporated 2016, now part of the Wealth Experts / Perspective group). The real firm has **publicly warned** that it "does not deal with Cryptocurrency" and that fraudsters abuse "the impersonated UK firm' name, details or FCA number." The scammers picked a genuine but low-profile firm so a quick check reassures the victim. The "Ministry of Finance and Statistics" and the "Finanzdirektor" are fabrications; Germany's real bodies are the Bundesfinanzministerium and BaFin, which do not audit private platform payouts or charge the public fees.

6.9 Visual & graphical red flags (you can see the fraud)

Even without the technical detail, the platform's own design gives it away (Exhibit D). A legitimate financial company pays for careful design; this kit was mass-produced and machine-translated with no human quality check:

- **Off-center button text.** The bottom-left "Abmelden" (logout) button text is not centered within the button shape, a basic layout error no real product ships.
- **Broken, machine-translated menu labels.** Left-hand items wrap mid-phrase with German fragments stranded onto the next line, for example "Überprüf enRechnung" and "Einstellung enSysteme," and the status column header is truncated to "Stan." This is automated translation dropped into a template with no layout review.
- **A leftover foreign word.** A column is labeled **"Platiti,"** Croatian/Serbian for "to pay," sitting inside an otherwise-German screen, a string left over from a different language pack in the same white-label kit.
- **Inconsistent capitalization.** Column headers are styled as capitalized headings except the last, "tatsächliche Rückerstattung," which is left lowercase, showing copy-paste with no proofreading.

In plain terms: real banks and exchanges do not ship screens with crooked buttons, half-translated menus, a random Croatian word, and sloppy capitalization. The design itself is a confession.

6.10 External footprint & reputation

Consistent with a fresh fraud domain: ScamAdviser 0/100, urlscan.io 0 scans, ChainAbuse 0 reports, no Trustpilot/Reddit/Web-of-Trust presence. For a 10-week-old site soliciting deposits, a near-zero footprint is the expected profile of a domain that will be burned and replaced (as the sibling dkmry.com already was).

7. SCAM CLASSIFICATION & PLAYBOOK

One integrated operation chaining a **task / gamified-job scam** (recruitment), **pig butchering** (build trust, then drain), and **advance-fee fraud** (the closing extraction). Where the client is:

#	STAGE	WHAT HAPPENED
0	Unsolicited add	Large Telegram group + private "task" channel (t.me/[REDACTED]); manufactured social proof.
1	Task scam	booking.com tasks, 18/day, small real payouts, reward ladder, "level up."
2	The hinge	"Trader tasks" 4/8/12/16 require depositing your own crypto. Task scam becomes pig butchering.
3	Fake exchange	dkmrf.com; rigged binary-options "trades" with fabricated balances.
4	Trust withdrawal	Small early payout allowed; "proof" it pays. Green light to deposit big.
5	Escalation	Deposit walls 2,560 to 4,820 EUR; 20 EUR "signup bonus" and scarcity ("few spots left") to push more.
6	**Slaughter (now)**	Forged insurance contract, "system rules," and a fake "payout password" to release funds. Advance-fee fraud.
7	Predicted next	More "tax / AML / Finanzdirektor activation" fees, urgency, then silence.
8	Predicted 2nd wave	"Recovery" service offers to get the money back for a fee. Same crew. A second scam (Section 13).

8. ATTRIBUTION: KNOWN, INFERRED, UNKNOWN, WHERE THE TRAIL DIES

What we know for sure VERIFIED

- Disposable, anonymously owned fake platform (created 2026-03-29) faking a market with a free Binance feed.
- Rigged binary-options product, a category banned for EU/German retail.
- Seal impersonates a real FCA firm that disclaims crypto; cited "ministry" and "Finanzdirektor" are fabricated.
- "Josie Bruns" is a reused recruiter alias; the booking.com task-scam is a heavily documented German-language pattern.
- 189 EUR went via PayPal to a private individual (money-mule signature); the scheme is active as of 2026-06-03.

What we infer (strong, not proven) INFERRED

- White-label, Chinese-origin "sha zhu pan" kit, localized to many markets; leftover strings "Platiti" (Croatian) and (Chinese) are localization artifacts, not proof of operator nationality.
- Persona photos are AI-generated or stolen. The PayPal transfer was "Friends & Family."

What is unknown / where the trail dies DEAD END

- **True operator identity and location** (Cloudflare + WHOIS privacy hide it).
- **Bitcoin deposit address(es)** (generated inside the logged-in dashboard; not visible to us). Without them, on-chain tracing cannot start.
- **Real people** behind "[money mule, name redacted]," "Josie Bruns," "Michael" (held by PayPal and Telegram), and the membership of the private Telegram channel.

9. INVESTIGATIVE LIMITS & WHAT IT WOULD TAKE TO GO FURTHER

OPEN QUESTION	WHAT IT WOULD TAKE
Trace the stolen Bitcoin	Deposit addresses + transaction hashes from the victim's wallet/dashboard, then chain-analysis and exchange cooperation. Typically a law-enforcement or licensed-investigator action.
Identify the mule / personas	PayPal and Telegram account records, released only to law enforcement via legal process.
Capture the Telegram channel	The +invite is perishable. Law enforcement should preserve it fast; metadata needs Telegram legal process.
Unmask the operators	Cloudflare origin + registrar + payment-provider records via subpoena / MLAT. Beyond OSINT.
Map the domain cluster & take it down	Passive-DNS / certificate pivoting across the "dkm**" family, plus abuse referrals to Cloudflare/registrar and FCA/BaFin warning listings. Available as a paid add-on.

10. RECOMMENDATIONS & VICTIM ACTION PLAN

Do these in order, today.

1. **Stop. Send nothing more.** Do not pay the "insurance," any "tax/fee," or the "payout password" demands. Do not sign the contract. Paying never releases funds.
2. **Report the PayPal payment as fraud now.** Report the 189 EUR to "[money mule, name redacted]," confirm whether it was Friends & Family, and ask PayPal to freeze the recipient. Speed beats the legal deadline.
3. **Call the funding bank/card** about a chargeback or SEPA recall if the PayPal payment was card- or bank-funded.
4. **Preserve evidence.** Screenshot the platform (account, withdrawal page, URL bar), save the contract and the channel link, export all Telegram chats, and list every payment (date, amount, wallet address, transaction ID). Back up off-device. Do not leave the group until captured.
5. **Recover the BTC deposit addresses** from the wallet/dashboard and submit them to ChainAbuse and law enforcement.
6. **File official reports** (Section 11), report @Josie6077, @M19951103 and the channel to Telegram, and notify the real the impersonated UK firm firm and the FCA so a clone warning can issue.

11. REPORTING DIRECTORY

JURISDICTION	BODY	CHANNEL
Germany	Police (Strafanzeige)	`portal.onlinewache.polizei.de`
	BaFin	`bafin.de (report a violation)`
	Verbraucherzentrale	`verbraucherzentrale.de/beschwerde`
USA	FBI IC3	`ic3.gov ("crypto job/task scam" + "pig butchering")`
	FTC	`reportfraud.ftc.gov`
UK	FCA (clone-firm)	`fca.org.uk firm checker / 0800 111 6768`
	Action Fraud	`actionfraud.police.uk`
Platforms	PayPal / Telegram / host abuse	`paypal.com report-fraud + funding bank · Telegram in-app report · registrar/Cloudflare abuse`

12. WARNING: THE SECOND SCAM (RECOVERY FRAUD)

After a loss like this, victims are almost always targeted by fake "fund recovery" services, frequently the same crew or affiliates, sometimes posing as lawyers, "blockchain investigators," or even the FBI/FCA. **Never pay an upfront fee to recover funds.** Real authorities never message you offering to retrieve money for a fee. Treat any unsolicited recovery offer as a second scam and block it. (The same impersonated firm name, "the impersonated UK firm," has itself been reused in crypto recovery scams.)

This was an industrialized criminal operation with paid actors, fabricated dashboards, and forged paperwork built to fool careful people. Falling for it is not a personal failing. The effective response is procedural: stop paying, preserve evidence, file reports, refuse all "recovery" offers.

APPENDIX A. INSURANCE CONTRACT TRANSLATION (GERMAN TO ENGLISH)

Source: Exhibit A. Translation by Viking Net Defense.

CRYPTO MARKET — INSURANCE CONTRACT (Versicherungsvertrag). Employee task code: [client email redacted]. "We provide you with an insurance contract for your platform account. Please take this contract seriously and pay careful attention to all details."

1. Investment plan. "An investment plan for the employee's account is to be created on the basis of really available 189 EUR and an appropriate profit target."

2. Compliance with instructions. "Employees must strictly follow the instructions of the investment manager. Private investments or withdrawals are strictly prohibited. A violation leads to cancellation of the order, blocking of the payout, and the sole liability of the employee."

3. Order profits and refund. "The profit of each order must exceed 30% of the base investment. Orders are randomly divided into 1 to 3 tranches; the last counts as a [refund order]. This policy applies only on the day of creation and is governed by the real conditions."

4. Double compensation for losses. "If the customer executes the order properly but the trader does not pay on time, the platform activates a double-compensation mechanism to protect the customer's rights. This compensation process is monitored and audited by the Ministry of Finance and Statistics. The mechanism also applies where losses or missing profits are the trader's fault."

5. Exclusion of payout on rule violation. "If an employee, for personal reasons, does not perform the tasks according to the platform's trading rules, the platform is entitled to provide no payout code. In that case the employee cannot make any withdrawals."

"*The final interpretation of this contract lies exclusively with our company, which also reserves the right to adapt and interpret the clauses according to the actual situation.*" [signature] [seal: a real, FCA-regulated UK wealth firm (name withheld), United Kingdom] Date: 03.06.2026

APPENDIX B. KEY TRANSLATIONS FROM THE NEW EVIDENCE

"System rules" from "Michael" (Exhibit M), summarized: investment data must not be shared; private investing or ignoring the mentor is forbidden; "we buy several cryptocurrencies at once"; the system gives 1 to 3 random "win orders," each requiring a prepayment / additional balance, the last being a "refund request"; no compensation for losses caused by violations; money transfers between participants are forbidden; "low creditworthiness" is threatened; and for a larger payout "contact the finance director to activate the payout channel, after which you receive a full refund. Reply OK."

Escalation message (handler): "Due to limited spots during the test phase (tens of thousands of employees daily), few places remain. So you do not miss the third trader task and permanent hiring, you receive a daily signup bonus of 20 EUR. Your video commission also rises to 6 EUR. Tell me immediately if you want the third trader task so I can reserve you a spot in the twelfth task." (Scarcity + bonus pressure to deposit.)

Payout gate (Exhibit N): "To process your payment, contact reception and share your payout password: [REDACTED]." (No real function; a pretext for the next fee.)

APPENDIX C. SELECTED SOURCES

- UK Companies House [reg. no. withheld] (the impersonated UK firm); the firm's public crypto disclaimer (Wealth Experts / Perspective)
- FCA: crypto-investment-scams, clone-firms, firm checker; Action Fraud
- ESMA binary-options retail prohibition (2018); BaFin permanent German ban (2019); BaFin betrügerische Handelsplattformen
- German Federal Ministry of Finance scam alerts; Verbraucherzentrale / Watchlist Internet / mimikama (task-scam & fake-trading)
- signal-arnaques.com #860816 / #862742 ("Josie Bruns" alias)
- CFTC / FBI binary-options & withdrawal-fee fraud; Proofpoint "Pig Butchers Join the Gig Economy"; Sophos sha-zhu-pan kits
- PayPal Friends & Family fraud / buyer-protection; Telegram private-invite documentation
- Live recon 2026-06-03: WHOIS, dig, crt.sh, ip-api, HTTP headers, page source

APPENDIX D. EVIDENCE EXHIBITS

> **Evidence exhibits withheld in this public sample.** The full client report includes all fourteen exhibits (screenshots of the fake platform, chats, and documents) with SHA-256 chain-of-custody. They are omitted here to protect the client and remove personal data.

Prepared by **Viking Net Defense**, a service of Viking Net LLC, San Antonio, Texas · vikingnetdefense.com · info@vikingnetllc.com. Based on open-source intelligence and victim-supplied materials as of 2026-06-03 (Public Sample). Findings labeled Verified, Inferred, or Unknown. Provided for the victim's protection and for submission to financial institutions and law enforcement. Not legal advice.