Confidencial

Relatório Análise On-chain

Arkham Intelligence

Sumário Executivo:

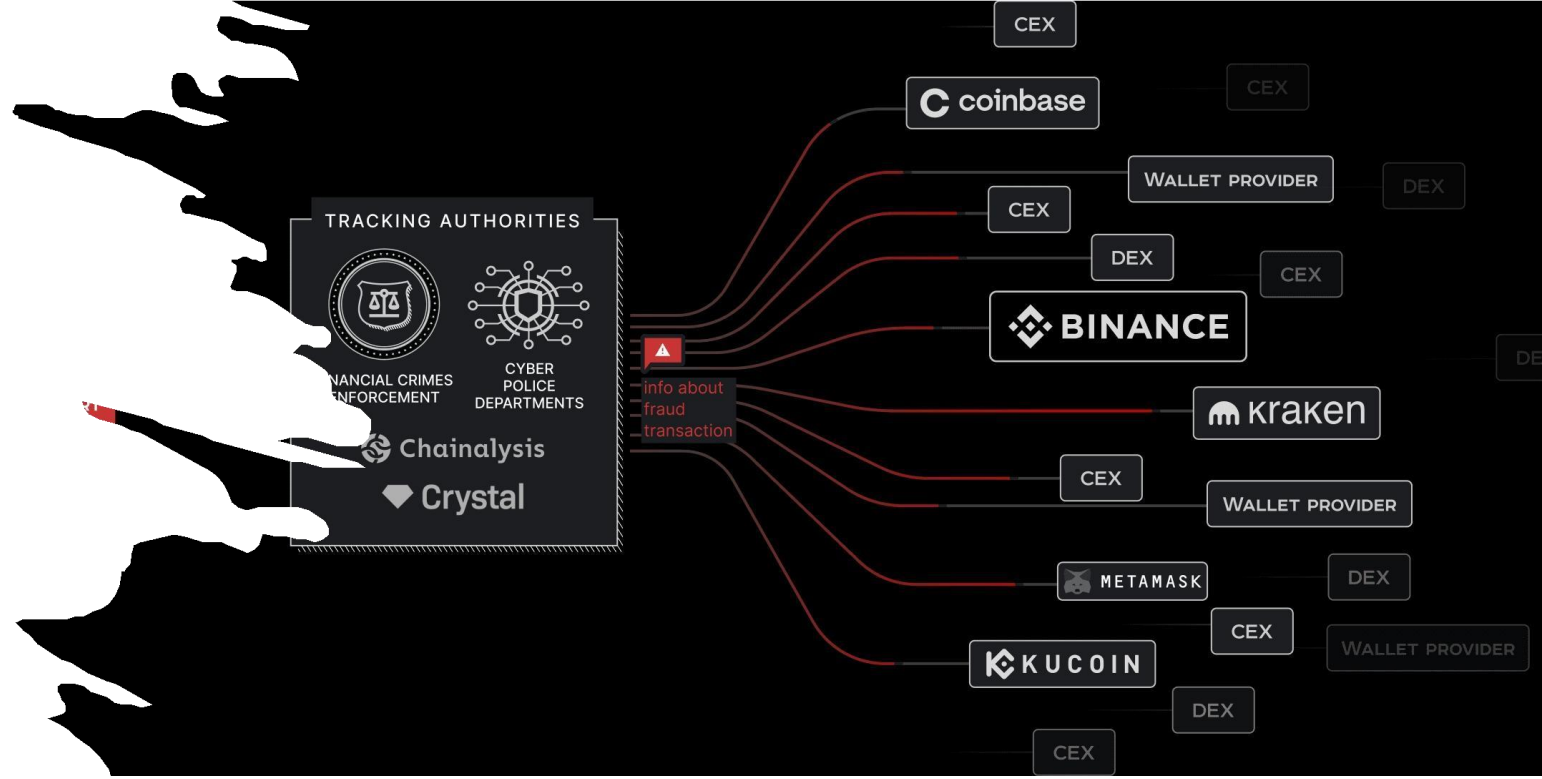
Protocolo de resposta ao incidente de roubo de Criptoativos.

Este relatório detalha o processo de atuação em resposta a fraudes envolvendo criptomoedas.

O procedimento inicia-se com a elaboração e o envio de um alerta para uma rede de mais de 200 entidades do setor, incluindo corretoras centralizadas (CEX), descentralizadas (DEX) e provedores de carteira.

A principal ação consiste em sinalizar os ativos digitais subtraídos, o que os torna inutilizáveis para transações futuras, bloqueando tentativas de liquidação por parte dos fraudadores. Paralelamente, prestamos auxílio integral à vítima para orientação em um registro de ocorrência policial qualificado. Para garantir a efetividade, operamos com um prazo de resposta de 72 horas. A investigação e o rastreamento das transações são realizados com o suporte de softwares de análise de blockchain e segurança financeira, como **Chainalysis**, **Crystal** ou **Arkhan**, permitindo o acompanhamento dos fundos através de múltiplos endereços e contas.

O serviço visa mitigar perdas e reforçar a segurança do ecossistema de criptoativos.



ARKHAM

Orientação Formal para Verificação de Autenticidade de Dispositivos LedgerData da Última Revisão: 14/05/2025.

0 introdução aos dispositivos de hardware da Ledger integram segurança em nível de hardware e software para proteger as chaves privadas do usuário contra um amplo espectro de vetores de ataque.

Este documento estabelece um protocolo de verificação formal para garantir que um dispositivo Ledger é autêntico e não foi adulterado, falsificado ou comprometido. A adesão estrita a estes procedimentos é imperativa para a segurança dos ativos digitais.

A verificação de autenticidade compreende uma série de inspeções físicas e uma verificação criptográfica fundamental realizada pelo software Ledger Live.2.0 Procedimentos de verificação preliminar antes da verificação por software, as seguintes inspeções manuais devem ser realizadas.

2.1. Verificação da Origem do Produto em Canais Autorizados:

A aquisição deve ser feita preferencialmente através de canais de venda oficiais para garantir a procedência do produto.

Site Oficial: **www.ledger.com**

Lojas Oficiais na Amazon: Incluindo EUA, Canadá, Reino Unido, Alemanha, França, Espanha, Itália, Japão, Austrália, Países Baixos, Polônia, Suécia, Turquia, Índia, Emirados Árabes Unidos, Bélgica, México e Cingapura.

Canais Não Oficiais: Dispositivos adquiridos de outros fornecedores exigem a execução rigorosa de todas as verificações subsequentes para validação de sua autenticidade.

2.2. Inspeção do conteúdo da embalagem:

A embalagem deve ser inspecionada para garantir que todos os componentes estejam presentes e em conformidade com o modelo adquirido.

Como exemplo, o conteúdo padrão para o modelo Ledger Stax é:

- 1x Dispositivo de hardware Ledger Stax
- 1x Cabo USB-C para USB-C (50 cm)
- 1x Envelope lacrado contendo uma folha de recuperação em branco
- 1x Guia de Início Rápido
- 1x Folheto de uso, cuidados e declaração regulatória

2.3. Verificação da Folha de Recuperação:

A folha de recuperação é um componente de segurança crítico.
A sua integridade deve ser validada da seguinte forma:

Condição da Folha: Deve estar completamente em branco.
Geração da Frase: A frase de recuperação de 24 palavras é gerada e exibida exclusivamente na tela do dispositivo Ledger durante o processo de configuração inicial.
ALERTA DE SEGURANÇA:
Se as folhas de recuperação contiverem qualquer palavra pré- impressa ou manuscrita, o dispositivo está comprometido e não deve ser utilizado.

A Ledger nunca fornece uma frase de recuperação ou código PIN por qualquer meio. A aceitação de credenciais pré-fornecidas resultará na perda de fundos. Contate o Suporte Ledger imediatamente em caso de anomalias.

2.4. Verificação do Estado Inicial do Dispositivo e do Código PIN

O comportamento do dispositivo ao ser ligado pela primeira vez é um indicador fundamental de sua autenticidade.

Ao ser ativado pela primeira vez, um dispositivo autêntico exibirá a tela de boas-vindas e guiará o usuário pelo processo de configuração inicial, que inclui a criação de um novo código PIN.

O usuário deve definir seu próprio PIN (recomenda-se 8 dígitos para segurança ótima).

ALERTA DE SEGURANÇA:

Se o dispositivo solicitar um código PIN existente na primeira utilização ou se um PIN for fornecido com a embalagem, o dispositivo não é seguro e deve ser considerado comprometido.

3.0 Procedimento de Verificação Criptográfica (Obrigatório)

Esta é a verificação de segurança mais importante, pois confirma criptograficamente a autenticidade do hardware.

3.1. Verificação de Autenticidade via Software Ledger Live

O aplicativo Ledger Live realiza uma verificação criptográfica para confirmar que o microcontrolador do dispositivo (Secure Element) é genuíno da Ledger.

Mecanismo: Dispositivos autênticos contêm uma chave secreta, implantada durante a fabricação. Somente um dispositivo genuíno pode usar essa chave para fornecer a prova criptográfica exigida pelo Ledger Live.

Execução: A verificação ocorre automaticamente durante o processo de configuração inicial do dispositivo no Ledger Live.
Verificações Posteriores: Uma verificação silenciosa é executada toda vez que o dispositivo é conectado à seção "Minha Ledger" no aplicativo.

Uma verificação manual também pode ser iniciada em Configurações > Ajuda > Configuração de Dispositivo.

3.2. Solução de Problemas de Conexão

Falhas na verificação podem ocorrer devido a problemas de conexão USB.

É vital garantir que cabos e portas USB estejam funcionando corretamente e que o dispositivo esteja desbloqueado com seu PIN durante o processo.

SUMARIO EXECUTIVO

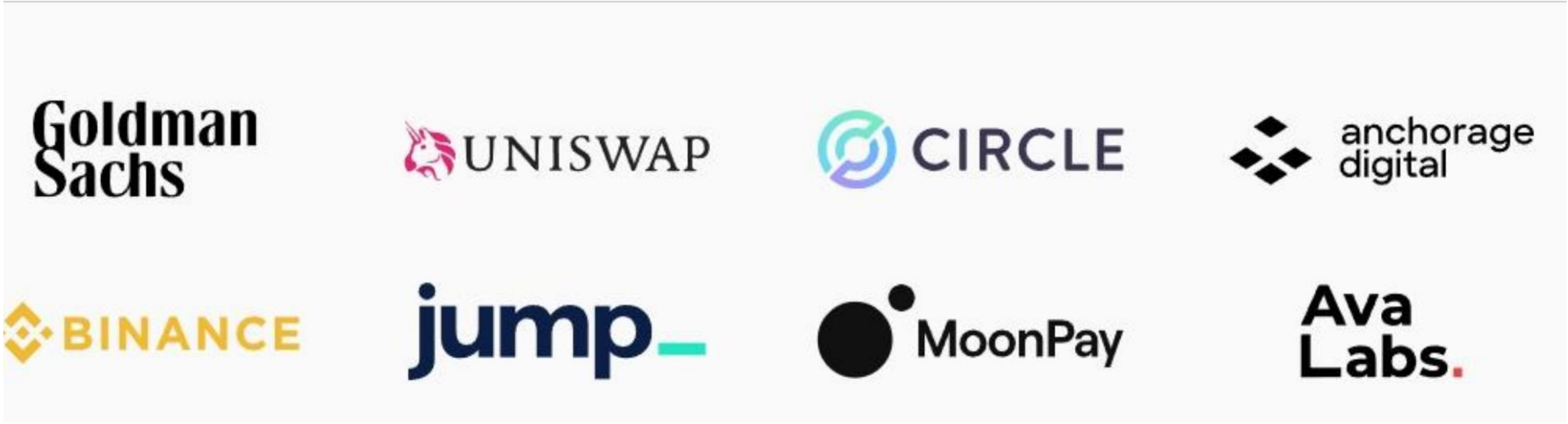
Análise Preliminar de Incidente de Segurança e Proposta de Investigação On-Chain ID do Caso: ZNT-202506-001

Cliente: **Confidencial**

Data do Incidente Principal: 26 de junho de 2025 (data estimada da exfiltração massiva)

Valor Total Exfiltrado: Aprox. $261,000.00 USD

Dispositivo Comprometido: Carteira de Hardware Ledger (ledger stax 2103, CÓDIGO SÉRIE 0UF447W02F)



Este documento constitui a análise preliminar de um incidente de segurança de alta gravidade envolvendo a exfiltração não autorizada de criptoativos de uma carteira de hardware Ledger, recentemente configurada pelo cliente.

O incidente, ocorrido entre 25 e 26 de junho de 2025, resultou na perda de aproximadamente $261,000.00 USD.

O cliente utilizava o dispositivo como uma carteira de tesouraria (treasury), com a intenção exclusiva de armazenamento a longo prazo (HODL), sem planejamento de transações de saída.

O objetivo deste relatório é:

a) Delinear a cronologia precisa dos eventos, desde a configuração do dispositivo até a subtração final dos fundos.
b) Formular as hipóteses investigativas iniciais sobre o vetor de ataque.
c) Estabelecer o escopo e os objetivos da análise on-chain subsequente, que será fundamental para o rastreamento dos ativos e para a compilação de um dossiê técnico robusto a ser apresentado às autoridades policiais competentes.

ARKHAM

Arkham Intelligence

Contexto e Cronologia Detalhada do Incidente

A reconstituição dos fatos, baseada no depoimento do cliente, aponta para uma sequência de eventos clara, que é crucial para a investigação. Aquisição e Configuração do Dispositivo (24 de junho de 2025)

O cliente realizou a aquisição de um dispositivo Ledger diretamente do site oficial do fabricante. Este é um passo de segurança recomendado e, a princípio, reduz a probabilidade de um ataque de cadeia de suprimentos (supply chain attack), onde o hardware é adulterado antes de chegar ao usuário final.

No dia 24 de junho de 2025, o cliente procedeu com a configuração inicial do dispositivo, gerando uma nova frase de recuperação de 24 palavras (seed phrase). A forma como esta frase foi manuseada e armazenada após a geração é um ponto crítico da investigação. Capitalização da Carteira e Primeiras Atividades (25 de junho de 2025)

No dia seguinte à configuração, o cliente iniciou o processo de capitalização da carteira, transferindo fundos para os endereços gerados pela Ledger. O propósito declarado era usar a carteira como um cofre digital para preservar capital, sem a intenção de realizar negociações ou transferências frequentes.

ARKHAM

Arkham Intelligence

Atividade Maliciosa Não Percebida e Exfiltração Final (25-26 de junho de 2025)

De forma crítica, o cliente não se atentou que, concomitantemente ou logo após as primeiras entradas, ocorreram transações de saída de baixo valor. Estas são, provavelmente, "transações de teste" realizadas pelo atacante para validar o controle sobre a carteira sem levantar suspeitas imediatas.

O evento culminou quando o cliente transferiu um montante significativo para a carteira, elevando o saldo para aproximadamente $260,000.00 USD. Pouco tempo depois desta grande transferência, a seguinte sequência de ataque foi executada:

Retirada de Validação: Uma transação de aproximadamente $1,000.00 USD foi executada pelo atacante.

Exfiltração Completa: Imediatamente após a confirmação da primeira retirada, o restante do saldo foi completamente drenado em uma ou mais transações subsequentes. Este padrão é clássico em ataques de carteira, onde o atacante aguarda a acumulação de um saldo substancial antes de realizar o saque final para maximizar o ganho e minimizar o tempo de reação da vítima.

Resposta do Cliente: Ao perceber a anomalia e a subsequente subtração do saldo, o cliente entrou em estado de urgência e buscou imediatamente assistência especializada para iniciar o processo de resposta ao incidente e recuperação.

ARKHAM

Arkham Intelligence

Hipótese Investigativa Inicial: Dado que o dispositivo foi adquirido de fonte oficial, a probabilidade de comprometimento do hardware é baixa. A investigação se concentra, portanto, na comprometimento da frase de recuperação de 24 palavras.

Os vetores de ataque mais prováveis incluem:

Phishing/Engenharia Social: O cliente pode ter sido induzido a inserir sua frase de recuperação em um site ou aplicativo falso que se passava por um serviço legítimo da Ledger ou de outra plataforma cripto.

Malware (Keylogger/Clipper): O computador ou smartphone utilizado durante a configuração ou para visualizar a seed phrase pode estar infectado com um malware que capturou as palavras ou que substituiu um endereço de destino no momento de uma transação.

Armazenamento Digital Inseguro: A frase de recuperação pode ter sido fotografada, digitada em um bloco de notas, ou salva em um serviço de nuvem ou e-mail, tornando-a vulnerável a hacks.

Exposição Física: A folha de recuperação física pode ter sido vista, fotografada ou copiada por um terceiro com acesso ao local de armazenamento.

ARKHAM

Arkham Intelligence

Objetivos da Análise On-Chain e Próximos Passos

A fase subsequente desta investigação será uma análise on-chain aprofundada, com os seguintes objetivos:

Mapear o Fluxo de Transações: Rastrear o movimento dos fundos exfiltrados desde a carteira do cliente, através de todos os endereços intermediários.

Identificar o Destino Final: Determinar se os fundos foram enviados para endereços de exchanges centralizadas (CEXs), serviços de mistura (mixers), protocolos DeFi, ou carteiras privadas.

Vincular Endereços a Entidades: Caso os fundos cheguem a uma CEX, iniciar o processo de contato com a plataforma para solicitar o congelamento dos ativos e a identificação do titular da conta (procedimento KYC/AML).

Coletar Evidências: Compilar todas as transações, endereços e timestamps em um relatório técnico detalhado que servirá como prova material para ser anexada ao boletim de ocorrência e entregue às autoridades policiais, capacitando-as a tomar as medidas legais cabíveis (como intimações judiciais para as exchanges).

LEDGER

$15.94 -3.1% Share

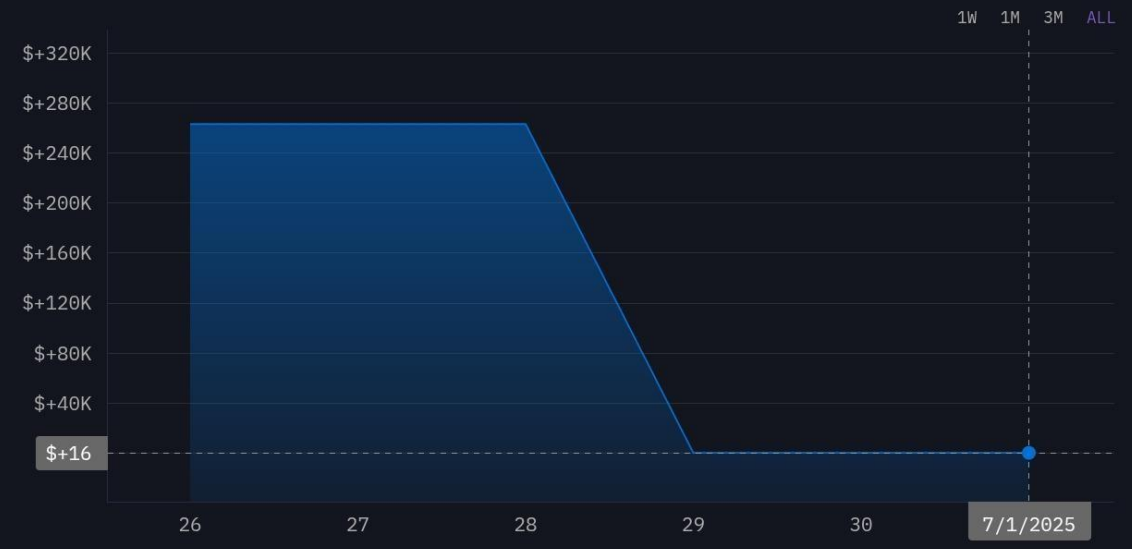
SHAREABLE ENTITY | ALL NETWORKS

Edit Entity | Create Alert + | Trace Entity | Visualize

PORTFOLIO | HOLDINGS BY CHAIN | PORTFOLIO ARCHIVE

ASSET	PRICE	HOLDINGS	VALUE
ETH	$2,415.22 -3.79%	0.00393 ETH	$9.49 -3.79%
BNB	$646.09 -1.84%	0.00996 BNB	$6.44 -1.84%
USDT	$1 ±0%	0.0145 USDT	$0.014 ±0%

BALANCES HISTORY | TOKEN BALANCES HISTORY | PROFIT & LOSS



EXCHANGE USAGE | TOP COUNTERPARTIES

6/24/2025 - 6/29/2025 (5 DAYS)

× USD ≥ $1

TRANSFERS | SWAPS | INFLOW | OUTFLOW

TIME	FROM	TO	VALUE	TOKEN	USD
4 days ago	LEDGER (0x84B)	RECEPTADOR 2 (0xCeA)	261.771K	USDT	$261.77K
4 days ago	LEDGER (0x84B)	RECEPTADOR 2 (0xCeA)	1K	USDT	$1K

TRANSACTION EXPLORER

NETWORK:	BNB CHAIN
TRANSACTION HASH:	0xd4b6521e9294161ade7823f42b5f23af7d65296a4b670e1fbb9043dfb152502f
STATUS:	COMPLETED
BLOCK:	#52083846
TIME:	6 days ago (25 Jun, 2025 16:48:07 UTC)
FROM:	MEXC: Hot Wallet (0x498)
TO:	LEDGER (0x84B)
VALUE	0.99999 BNB ($644.24)
TOTAL FEE	0.000042 BNB ($0.027)
GAS PRICE	2 GWEI
GAS LIMIT & USAGE	50,000 | 21,000

Default | Analyze

EXCHANGE USAGE | TOP COUNTERPARTIES

6/24/2025 - 6/29/2025 (5 DAYS)

DEPOSITS

EXCHANGE	VALUE
Total	$636.48 (100%)
HITBTC	$636.48 (100%)

WITHDRAWALS

EXCHANGE	VALUE
Total	$262.79K (100%)
MEXC	$262.79K (100%)

Analyze

BORROWS & LOANS

NET VALUE

$0 +0.00%

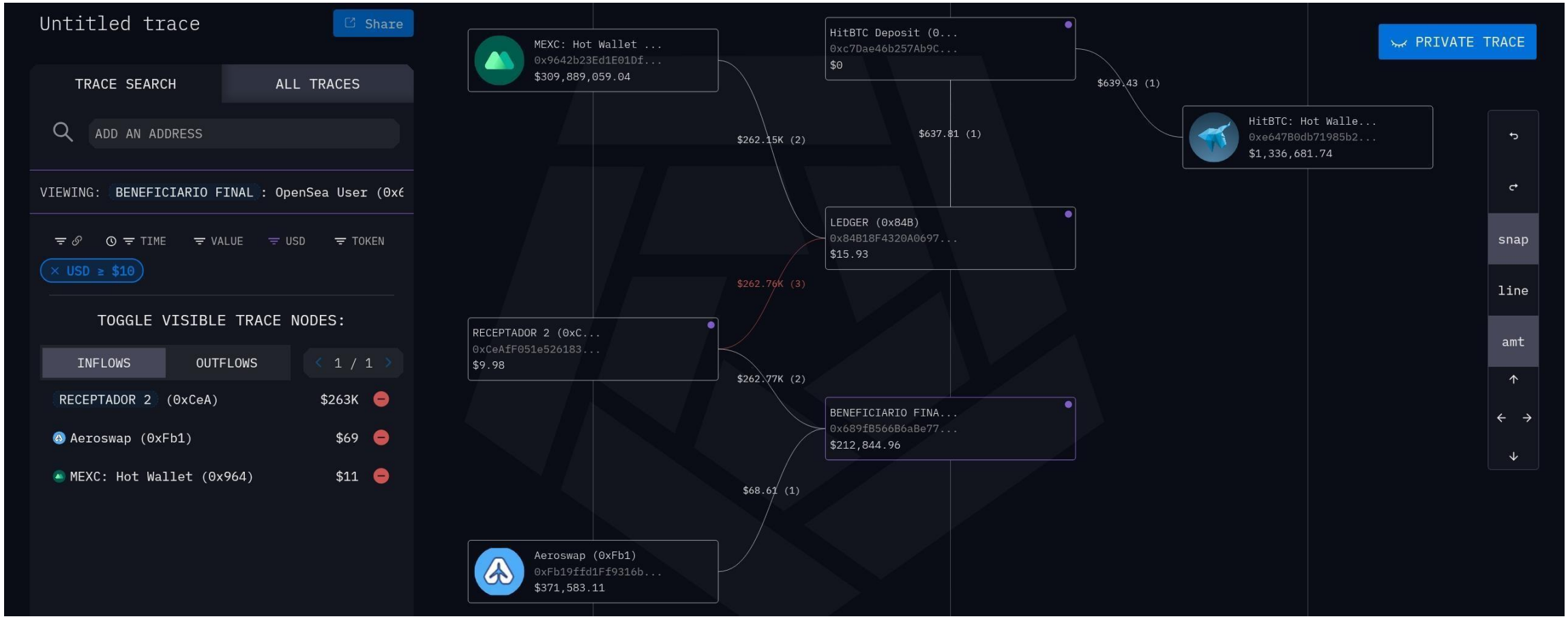
LARGEST POSITIONS

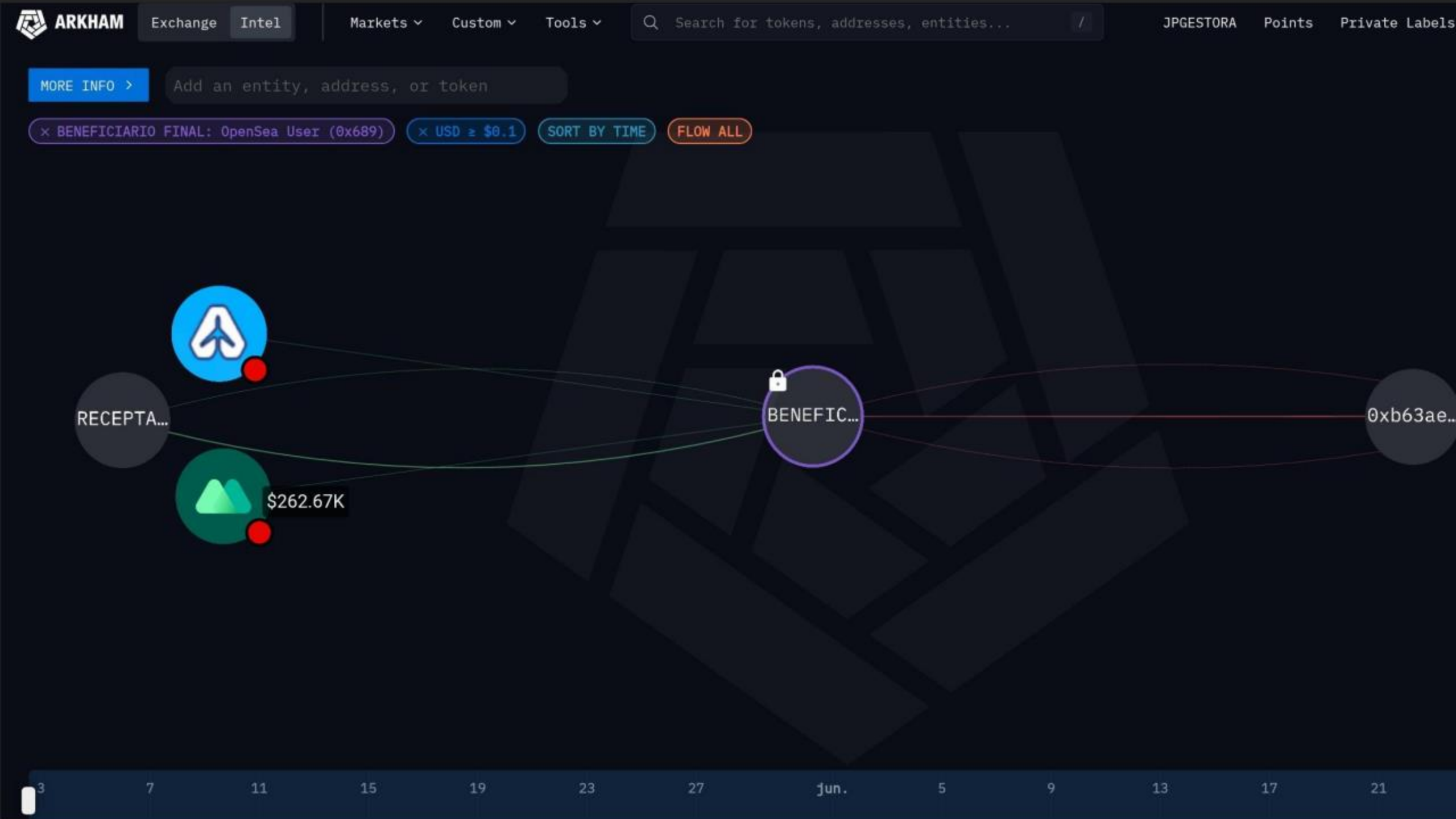
PLATFORM	USD VALUE	POSITIONS	NETWORK

USD ≥ $1

TRANSFERS | SWAPS | INFLOW | OUTFLOW

TIME	FROM	TO	VALUE	TOKEN	USD
4 days ago	LEDGER (0x84B)	RECEPTADOR 2 (0xCeA)	261.771K	USDT	$261.77K
4 days ago	LEDGER (0x84B)	RECEPTADOR 2 (0xCeA)	1K	USDT	$1K
4 days ago	RECEPTADOR 2 (0xCeA)	LEDGER (0x84B)	0.0042	ETH	$10.17
6 days ago	MEXC: Hot Wallet (0x…	LEDGER (0x84B)	262.047K	USDT	$262.05K
6 days ago	MEXC: Hot Wallet (0x…	LEDGER (0x84B)	99	USDT	$99
6 days ago	0xA3222357a0eCCF60C73…	LEDGER (0x84B)	625.468	USDT	$625.47
6 days ago	LEDGER (0x84B)	HitBTC Deposit (0xc7D)	0.99	BNB	$637.81
6 days ago	MEXC: Hot Wallet (0x…	LEDGER (0x84B)	1	BNB	$644.24


Untitled trace
Share
TRACE SEARCH
ALL TRACES
ADD AN ADDRESS
VIEWING: BENEFICIARIO FINAL : OpenSea User (0x6
TIME
VALUE
USD
TOKEN
USD ≥ $10
TOGGLE VISIBLE TRACE NODES:
INFLOWS
OUTFLOWS
1 / 1
RECEPTADOR 2 (0xCeA) $263K
Aeroswap (0xFb1) $69
MEXC: Hot Wallet (0x964) $11
MEXC: Hot Wallet ...
0x9642b23Ed1E01Df...
$309,889,059.04
HitBTC Deposit (0...
0xc7Dae46b257Ab9C...
$0
$639.43 (1)
HitBTC: Hot Walle...
0xe647B0db71985b2...
$1,336,681.74
PRIVATE TRACE
$262.15K (2)
$637.81 (1)
LEDGER (0x84B)
0x84B18F4320A0697...
$15.93
$262.76K (3)
RECEPTADOR 2 (0xC...
0xCeAfF051e526183...
$9.98
$262.77K (2)
BENEFICIARIO FINA...
0x689fB566B6aBe77...
$212,844.96
$68.61 (1)
Aeroswap (0xFb1)
0xFb19ffd1Ff9316b...
$371,583.11
snap
line
amt


ARKHAM
Exchange
Intel
Markets
Custom
Tools
Search for tokens, addresses, entities...
/
JPGESTORA
Points
Private Labels
MORE INFO >
Add an entity, address, or token
× BENEFICIARIO FINAL: OpenSea User (0x689)
× USD ≥ $0.1
SORT BY TIME
FLOW ALL
RECEPTA...
$262.67K
BENEFIC...
0xb63ae...
3
7
11
15
19
23
27
jun.
5
9
13
17
21

BENEFICIARIO FINAL

$212,844.95 -0.00011%

Share

SHAREABLE ENTITY

ALL NETWORKS

Edit Entity | Create Alert + | Trace Entity | Visualize

Click to copy - anyone with the link can view

ORTFOLIO | HOLDINGS BY CHAIN | PORTFOLIO ARCHIVE

PRICE	HOLDINGS	VALUE
$1 ±0%	212.839K USDT	$212.84K ±0%
$2,410.79 -3.59%	0.00251 ETH	$6.04 -3.59%

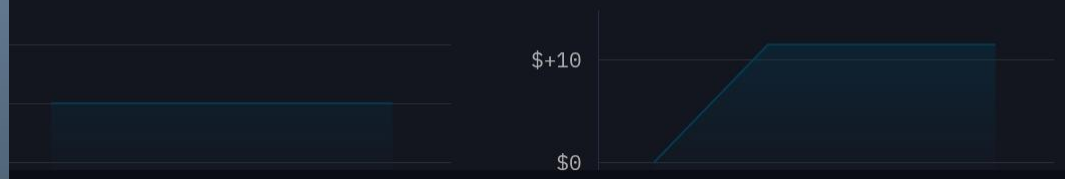
BALANCES HISTORY | TOKEN BALANCES HISTORY | PROFIT & LOSS

1W 1M 3M ALL

EXCHANGE USAGE | TOP COUNTERPARTIES

6/26/2025 - 6/29/2025 (3 DAYS)

DEPOSITS WITHDRAWALS



USD ≥ $1

TRANSFERS | SWAPS | INFLOW | OUTFLOW

TIME	FROM	TO	VALUE	TOKEN	USD
3 days ago	BENEFICIARIO FINAL: 0…	OpenSea User (0xa54)	0.00206	ETH	$5
3 days ago	BENEFICIARIO FINAL: 0…	OpenSea User (0xa54)	49.99K	USDT	$49.99K

CHAT ROOM: BENEFICIARIO FINAL

EXCHANGE USAGE | TOP COUNTERPARTIES

6/26/2025 - 6/29/2025 (3 DAYS)

DEPOSITS

EXCHANGE	VALUE
Total	$0 (0%)

WITHDRAWALS

EXCHANGE	VALUE
Total	$11.41 (100%)
MEXC	$11.41 (100%)

USD ≥ $1

TRANSFERS | SWAPS | INFLOW | OUTFLOW

TIME	FROM	TO	VALUE	TOKEN	USD
3 days ago	BENEFICIARIO FINAL : O…	OpenSea User (0xa54)	0.00206	ETH	$5
3 days ago	BENEFICIARIO FINAL : O…	OpenSea User (0xa54)	49.99K	USDT	$49.99K
3 days ago	BENEFICIARIO FINAL : O…	OpenSea User (0xa54)	10	USDT	$10
4 days ago	RECEPTADOR 2 (0xCeA)	BENEFICIARIO FINAL : O…	262.671K	USDT	$262.67K
4 days ago	RECEPTADOR 2 (0xCeA)	BENEFICIARIO FINAL : O…	100	USDT	$100
4 days ago	BENEFICIARIO FINAL : O…	0xb63ae19F00C4c55310ECa…	1	USDT	$1
4 days ago	MEXC: Hot Wallet (0x…	BENEFICIARIO FINAL : O…	0.00471	ETH	$11.38
5 days ago	Aeroswap (0xFb1)	BENEFICIARIO FINAL : O…	68.61	USDT	$68.61

TRANSACTION EXPLORER

NETWORK:	ETHEREUM
TRANSACTION HASH:	0x2cae1144f65adaf8588ab34e2c6eec4580593e8faa311b9a96210f31fafba400
STATUS:	COMPLETED
BLOCK:	#22799488
TIME:	4 days ago (28 Jun, 2025 00:55:59 UTC)
FROM:	RECEPTADOR 2 (0xCeA)
TO:	Tether: Tether USD (USDT) (0xdAC)
VALUE	0 ETH ($0)
TOTAL FEE	0.000096790499815464 ETH ($0.23)
GAS PRICE	2.342404584 GWEI
GAS LIMIT & USAGE	46,237 | 41,321

Default | Analyze

TOKEN TRANSFERS (1)

TIME	FROM	TO	VALUE	COIN	USD
4 days ago	RECEPTADOR 2 (0xCeA)	BENEFICIARIO FINAL : OpenSea User (0x6…	262.671K	USDT	$262.67K

ARKHAM

Arkham Intelligence

RELATÓRIO DE ATIVIDADE SUSPEITA E SOLICITAÇÃO DE MEDIDAS INVESTIGATIVAS.

Assunto: Solicitação de investigação, rastreamento de ativos, congelamento de fundos e cooperação internacional referente a endereço de blockchain envolvido em atividade ilícita.

1. Introdução

Este relatório tem como finalidade apresentar informações detalhadas sobre atividades fraudulentas e de lavagem de dinheiro, bem como solicitar formalmente a intervenção desta autoridade para a adoção das medidas legais cabíveis. O objetivo é viabilizar a identificação do autor do delito, bloquear e reaver os ativos obtidos ilicitamente, e impedir a continuidade da atividade criminosa.

2. Descrição dos Fatos

O indivíduo, beneficiário final e proprietário do endereço de blockchain na rede Ethereum 0x689fB566B6aBe77682aCD96e28E61b12a40F946C, realizou uma operação com o claro intuito de ocultar a origem de recursos possivelmente ilícitos.

ARKHAM

Arkham Intelligence

A ação consistiu na conversão dos criptoativos mantidos no referido endereço em um Token Não Fungível (NFT) por meio da plataforma OpenSea. Esta tática é frequentemente utilizada por criminosos para dificultar o rastreamento e a liquidação de fundos, configurando um forte indício de lavagem de dinheiro.

3. Plataformas e Entidades Envolvidas

Para o avanço da investigação, é crucial a colaboração das seguintes entidades:

Corretora (Exchange): A corretora MEXC (foi identificada como um ponto de passagem potencial dos recursos ou como a plataforma de origem do indivíduo. A obtenção dos dados de KYC (Know Your Customer) junto a esta empresa é uma etapa indispensável para a identificação do beneficiário final dos valores.

Marketplace de NFT: A plataforma OpenSea (https://opensea.io/) foi utilizada para a conversão dos ativos, e seus registros internos podem conter informações vitais sobre a conta do usuário e o NFT em questão.

Protocolos de Finanças Descentralizadas (DeFi): Plataformas como a Uniswap e outras são frequentemente utilizadas para a etapa final de liquidação dos ativos.

Arkham Intelligence

4. Medidas Preliminares Adotadas

Com o intuito de mitigar os danos e alertar a comunidade global, as seguintes ações já foram executadas:

Denúncia Pública em Plataforma Especializada: Foi efetuado um relatório detalhado na Chainabuse, a principal plataforma global para denúncia de atividades maliciosas com criptomoedas. Esta ação torna o endereço publicamente marcado como fraudulento para milhões de usuários e serviços integrados

Reporte de Phishing ao Etherscan: Foi submetido o formulário de "Phishing Report" ao explorador de blocos Etherscan, solicitando que o endereço seja devidamente sinalizado como malicioso, o que gera um alerta para todos que interagirem com ele.

5. Solicitações Formais

Diante do exposto, solicita-se respeitosamente a esta autoridade que adote as seguintes providências em caráter de urgência:

Requisição Judicial de Dados (KYC): Expedir ofício judicial à corretora MEXC e outras que se façam necessárias durante a investigação, para que forneçam os dados cadastrais completos (KYC/AML) vinculados ao endereço **0x689fB566B6aBe77682aCD96e28E61b12a40F946C** e às transações relacionadas.

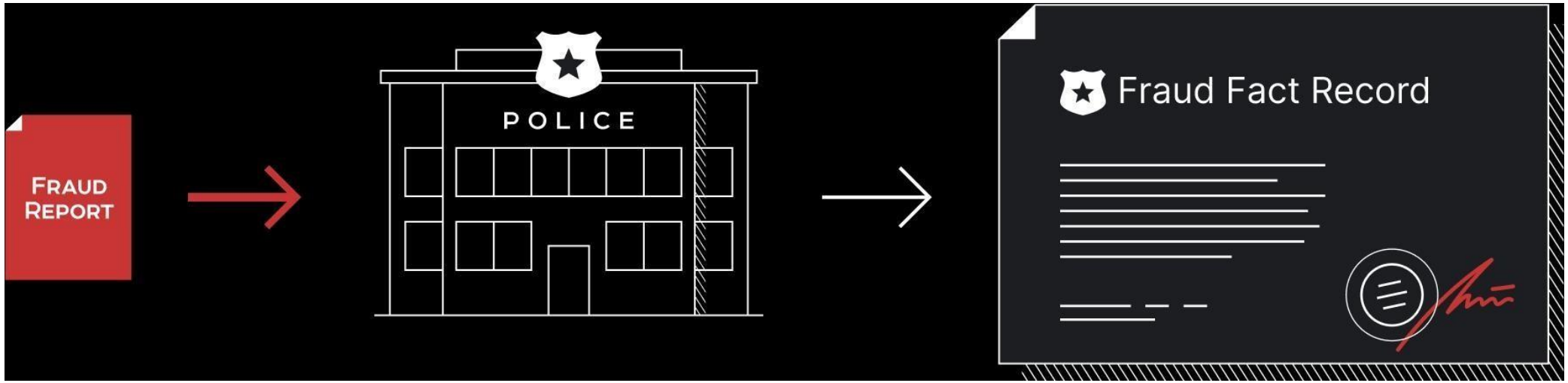
ARKHAM

Arkham Intelligence

Bloqueio e Congelamento de Ativos: Iniciar os procedimentos para o congelamento imediato dos ativos (o NFT e quaisquer outros criptoativos) presentes no endereço supracitado. Se necessário, que sejam acionados os mecanismos de cooperação jurídica internacional para garantir a eficácia da medida em jurisdições estrangeiras.

Inclusão em Listas Restritivas (Blacklists): Requerer formalmente a inclusão do endereço em listas de sanções e fraudes utilizadas globalmente. Esta medida é crucial para impedir a negociação, venda ou liquidação dos ativos em mais de 200 instituições financeiras, corretoras centralizadas e protocolos descentralizados (como Uniswap), asfixiando economicamente a capacidade de ação do criminoso.

Conclusão: A rápida atuação desta autoridade é fundamental para impedir a dissipação dos valores, garantir o ressarcimento da vítima e responsabilizar criminalmente o autor. Colocamo-nos à inteira disposição para fornecer informações adicionais e colaborar ativamente com o andamento da investigação.



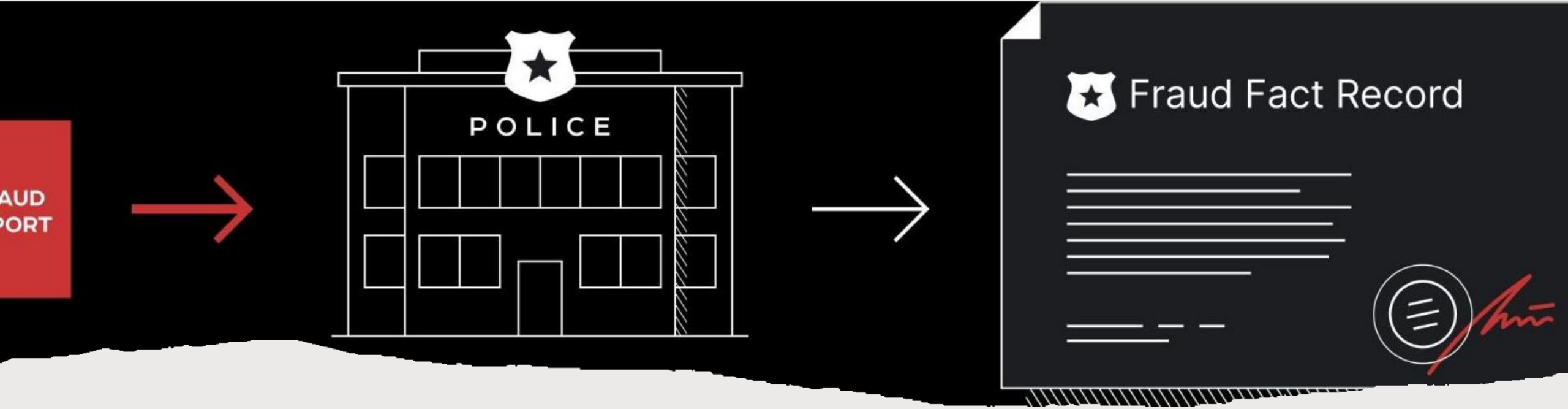
Delegacias Virtuais: O Guia Completo para Registrar Ocorrências Policiais Online no Brasil

Em uma era cada vez mais digital, a segurança pública também se moderniza.

Cidadãos de todo o Brasil já podem registrar diversas ocorrências policiais sem sair de casa, utilizando as delegacias virtuais.

Estes portais online, mantidos pelas Polícias Civis de cada estado, oferecem um meio rápido e acessível para a comunicação de crimes e outros fatos, otimizando o tempo do cidadão e dos agentes de segurança.

Abaixo, um guia completo com os links para o registro de ocorrências em todos os estados brasileiros



Distrito Federal, além de informações sobre o portal nacional e a atuação da Polícia Federal.

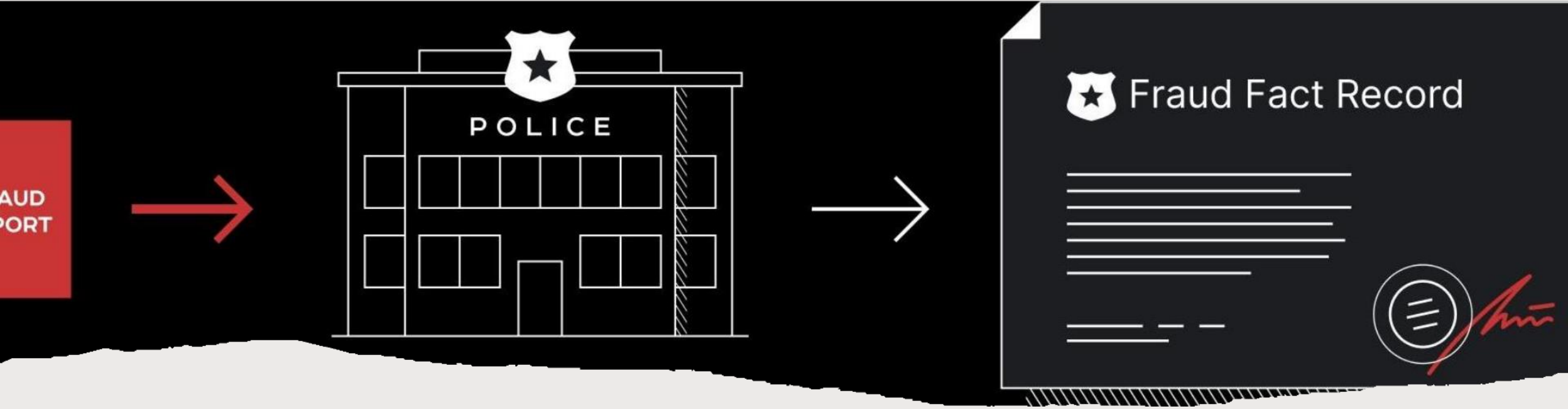
Portal Nacional - Delegacia Virtual do Ministério da Justiça e Segurança Pública

Uma iniciativa para unificar o acesso à justiça, a Delegacia Virtual do Ministério da Justiça e Segurança Pública (DEVIR) atende a diversos estados.

Através de um único portal, o cidadão pode selecionar sua localidade e ser direcionado para o sistema correspondente.

Link: **https://delegaciavirtual.sinesp.gov.br**

Este portal integra o registro de ocorrências para os seguintes estados: Acre, Alagoas, Amapá, Amazonas, Bahia, Maranhão, Piauí, Rio Grande do Norte, Rondônia, Roraima, Sergipe e Tocantins.



Delegacias Virtuais por Estado: Para os estados que não estão integrados ao portal nacional, o registro de ocorrência online é feito através de seus próprios sites.

Confira a lista:

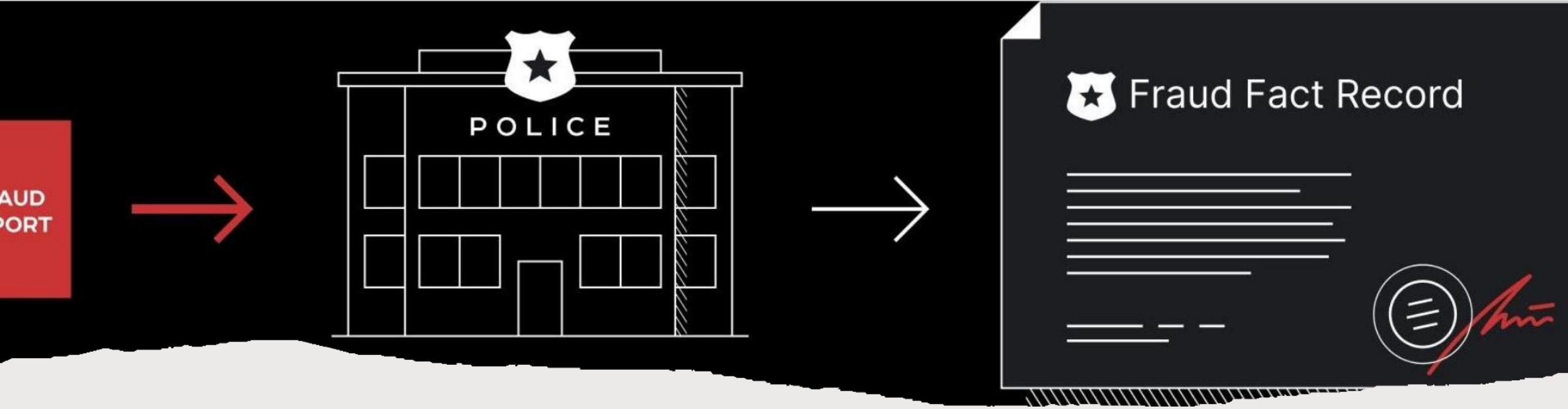
Ceará: https://www.delegaciaeletronica.ce.gov.br - **Distrito Federal:** O registro é feito através do portal nacional da Delegacia Virtual. **Espírito Santo:** https://delegaciaonline.sesp.es.gov.br/ - **Goiás:** https://www.policiacivil.go.gov.br/delegacia-virtual

Mato Grosso: https://portal.sesp.mt.gov.br/delegacia-virtual/ - **Mato Grosso do Sul**: http://devir.pc.ms.gov.br/

Minas Gerais: https://delegaciavirtual.sids.mg.gov.br/ - **Pará:** https://www.delegaciavirtual.pa.gov.br/ - **Paraíba:** https://www.delegaciaonline.pb.gov.br/ - **Paraná:** https://www.policiacivil.pr.gov.br/BO - **Pernambuco:** O registro é feito através do portal nacional da Delegacia Virtual. - **Rio de Janeiro:** https://delegaciaonline.pcivil.rj.gov.br/ - **Rio Grande do Sul:** https://www.delegaciaonline.rs.gov.br/

Santa Catarina: https://delegaciavirtual.sc.gov.br/ - **São Paulo:** https://www.delegaciaeletronica.policiacivil.sp.gov.br/Polícia Federa

Até o momento, a Polícia Federal não dispõe de um sistema de delegacia virtual para o registro de ocorrências pela população em geral, similar aos sistemas das polícias civis estaduais.



A apuração de crimes de competência federal, como tráfico internacional de drogas, crimes contra o sistema financeiro nacional e outros previstos em lei, geralmente se inicia a partir de denúncias ou por meio de investigações próprias da instituição.

Em muitos casos, o registro inicial de um fato que possa ser de atribuição federal pode ser feito na delegacia de polícia civil, que, por sua vez, pode encaminhar o caso à Polícia Federal se a competência for confirmada.Importante:

A comunicação falsa de crime é crime, previsto no Código Penal Brasileiro.

Ocorrências graves, que exigem a presença imediata da polícia, como crimes em andamento ou que envolvam violência, devem ser comunicadas imediatamente através dos telefones de emergência 190 (Polícia Militar) ou outros números de emergência locais.

Cada portal estadual possui suas próprias regras sobre quais tipos de ocorrências podem ser registradas online. Geralmente, são aceitos casos de menor potencial ofensivo, como furtos, perda de documentos, acidentes de trânsito sem vítimas, entre outros. Verifique as orientações no site correspondente.

JP Gestora de Fundos

compliance@jetprive.com.br