COLL
ISION
LESS

THREAT INTELLIGENCE REPORT

What a Kidnapper Sees Before Taking Action

How Do Your Dots Connect?

THREAT ASSESSMENT SERIES JARED GABBAY 2026

© 2026 Collisionless Global Technology Services Inc.

TABLE OF CONTENTS

What’s Inside

01	SUMMARY	Executive Summary	3
02	SCOPE	Scope and Analytic Frame	5
03	THREAT ACTORS	Threat Actors and the Risk-Reward Decision	7
04	QUALIFICATION	Target Qualification	10
05	EXPOSURE	Exposure Accumulates Across Sources	12
06	CONVERGENCE	How Information Becomes Useful	14
07	REMOVAL	Removal Does Not Resolve Risk	16
08	REMEDIATION	Remediation	18
09	CONCLUSION	Conclusion	20

© 2026 Collisionless Global Technology Services Inc.

Executive Summary

Onchain exposure is often discussed as a financial security problem: a wallet is identified, a balance becomes visible, and the owner becomes more vulnerable to fraud or theft. That framing is incomplete. Once blockchain activity is credibly connected to a real person, it can also influence decisions in the physical world. It may help someone form a belief about wealth, decide that a person is worth further attention, identify other people who could be pressured, and conclude that violence might produce value that can be transferred quickly. The resulting risk is not created by the blockchain alone. It emerges from the connection between financial activity and public information about identity, location, routines, relationships, business roles, travel, and access.

> *The central judgment of this assessment is that physical risk depends less on verified net worth than on a bad actor's perception of reward, access, and likelihood of payment.*

An opportunistic offender may require little more than a visible wealth signal, a current location, and a belief that a phone or device provides immediate access. A coordinated crew usually needs enough confidence to justify additional people and logistics. An organized domestic or transnational network may spend substantial time and money when the perceived payoff is exceptional. A believed $100 million payoff can support an investment of time and resources that would make little sense for a $20,000 payoff. There is no universal threshold because the decision is comparative. Expected reward is weighed against cost, uncertainty, exposure to law enforcement, and the actor's capabilities.

Public information becomes dangerous through accumulation. A professional biography may establish identity, a company role may imply wealth, a public wallet association may appear to confirm it, an event announcement may place the person in a specific city, and a family or vendor account may reveal how the person can be reached. Their value comes from corroboration and convergence. Separate facts that appear to agree give an actor confidence, while facts that become current at the same moment can turn a general profile into an immediate opportunity. The process can operate even when the underlying assumptions are wrong. A stale wallet label, exaggerated social-media persona, misunderstood business role, or rumor about custody can motivate real violence if the resulting story is persuasive enough.

This distinction between evidence and belief is essential. Tracing follows value visible on a blockchain. Attribution connects that activity to a person or organization. Ownership asks who benefits from the assets; control asks who can move them; present control asks whether that remains true now. A careful investigator would not collapse these conclusions. A criminal may.

© 2026 Collisionless Global Technology Services Inc.

A public association that would not withstand formal evidentiary scrutiny can still create a believable story about wealth and access.

Removal is useful but does not restore a blank slate. Historical blockchain records remain, copied data persists, public claims are repeated, and later behavior can reconnect identities meant to be separated. Effective remediation is therefore measured not by how many records disappear, but by whether the strongest pathways become less current, credible, connected, and actionable. The objective is to change the actor's economics: reduce confidence in the reward, reduce access to the person and related people, increase the time and uncertainty required to act, create friction around the movement of value, and prepare the household and organization to respond before an incident occurs.

© 2026 Collisionless Global Technology Services Inc.

Scope and Analytic Frame

This assessment examines the point at which public identity, apparent wealth, onchain activity, physical access, and human relationships combine into a credible physical security concern. Kidnapping is the most severe expression, but the same exposure can support robbery, extortion, home invasion, coercion, impersonation, or pressure against a family member, employee, or business partner. The purpose is defensive: to explain the judgments that matter when evaluating exposure and identify principles that reduce it. The mechanics of locating, surveilling, approaching, or coercing a target are intentionally excluded, as are named tools and reproducible procedures.

The assessment draws on patterns seen in investigations, undercover work, financial tracing, source handling, surveillance, case preparation, and public reports of violence involving cryptocurrency holders and other visibly affluent victims. The meaningful risk rarely resides in one spectacular piece of information. It develops across domains that the subject experiences as separate, but an outsider does not. Personal, professional, financial, family, and travel information may sit in different accounts and databases yet still describe the same person.

> *A defensive review must therefore examine the connected profile rather than treat each platform, wallet, address, or account as an independent problem.*

Undercover work is particularly relevant because it requires disciplined attention to identity management. An identity is sustained not by a name alone, but by a coherent pattern of conduct, relationships, history, language, and repeated details. The same principle works in reverse when someone attempts to reduce exposure. Changing a username, email address, company entity, or wallet does not create meaningful separation if behavior and relationships continue to connect the old identity to the new one. The test is whether an informed outsider can still form a credible bridge between them; you might buy a new car but keep the old bumper sticker.

© 2026 Collisionless Global Technology Services Inc.

Law enforcement experience also reinforces the need to distinguish observation, inference, corroboration, and proof. Affidavits and investigative reports cannot treat an assumption as fact merely because it is plausible or widely repeated. The physical threat environment is less disciplined. An offender may proceed on rumor, exaggeration, or a mistaken conclusion if it appears credible enough relative to the expected reward. A defensive assessment must therefore preserve evidentiary distinctions while also examining the harm that can arise from false attribution. It is not enough to say that a claim about wealth or control is unproven. The relevant question is whether that claim could influence someone who is willing to act without proof.

© 2026 Collisionless Global Technology Services Inc.

Threat Actors and the Risk-Reward Decision

The word *kidnapper* can conceal more than it explains. Threat actors range from impulsive local offenders to access-enabled insiders, small, coordinated crews, and organized networks capable of operating across jurisdictions. These categories are not rigid, and participation can be hybrid. A local person may notice an opportunity, an acquaintance may validate the subject's identity or routine, another person may provide transportation or introductions, and a separate group may handle the proceeds. No single participant needs a complete picture; a small disclosure can supply one missing piece of confidence, access, or capability.

At the opportunistic end of the spectrum, the decision threshold can be low. The actor may already be in the same city, venue, or social environment and need only a visible indication of wealth and a moment of perceived access. A social-media post that promotes an expensive lifestyle and places the subject in a city in real time can create a sufficiently attractive opportunity for someone nearby. The expected return only needs to appear large relative to the effort required and the risk the offender believes he is taking. Such an actor may also be poorly informed about how digital assets are controlled. Defensive planning cannot assume the offender understands multisignature arrangements, institutional custody, delays, or that a visible balance may not belong to the person associated with it.

An acquaintance, employee, contractor, former associate, romantic partner, vendor, or household service provider occupies a different position. Familiarity reduces the cost of collecting information and may give the actor confidence about a residence, vehicle, routine, device, family relationship, or apparent custody arrangement. Proximity does not establish reliability; a person close to the subject may still be biased, mistaken, out of date, or deceptive. Nevertheless, an offender may treat that person's access as corroboration. The insider need not participate in violence. A limited disclosure about schedule, household composition, or perceived control can make a public profile substantially more useful to someone else.

Small, coordinated groups incur more cost. Additional participants, communications, transportation, planning, and division of proceeds create more failure points and greater law-enforcement exposure. As those costs rise, so does the amount of confidence normally required before acting. Public cases involving affluent households show that offenders have selected victims after displays of wealth, collectible property, or expensive lifestyles on social media. Those examples matter even when cryptocurrency was not involved because the selection logic is not new. Digital assets change the perceived reward: unlike a vehicle, watch, or artwork, cryptocurrency may appear capable of being transferred without storage, resale, or a conventional intermediary.

© 2026 Collisionless Global Technology Services Inc.

Organized domestic and transnational networks sit farther along the same economic continuum. Their threshold for committing resources is higher, but so is their ability to absorb uncertainty, wait for a favorable opportunity, recruit specialists or local participants, travel, and move proceeds through multiple jurisdictions. A believed nine-figure payoff can justify months of attention and a meaningful financial outlay. Public cryptocurrency cases have demonstrated coordination across digital compromise, physical observation, travel, violence, and laundering. A widely reported French case in which Ledger co-founder David Balland and his partner were abducted for ransom illustrates that structured groups can treat a person's industry role and apparent access as the basis for a planned physical operation[1]. It does not establish that most attacks against cryptocurrency holders are transnational; it establishes that exceptional perceived value can attract actors with exceptional reach.

Coinbase's 2026 proxy statement reported $7.64 million in 2025 costs for CEO Brian Armstrong's personal security, up from $6.24 million in 2024 and $3.70 million in 2023[2]. Armstrong is an unusual case, not a general benchmark. Even so, the figures show how a major exchange prices this risk and treats executive security as a material, recurring expense. The defensive logic is straightforward: higher perceived value can require greater protective resources.

Organized crime should not be imagined only as a neat hierarchy. A more useful model is often a network of contributors who provide access, introductions, transportation, violence, money movement, or local knowledge. The final act may be crude even when preparation reflects considerable capability. Conversely, three people acting together are not automatically part of a durable criminal organization. Protective decisions should follow observed capability, persistence, coordination, and resources rather than dramatic labels. This matters because overstating sophistication wastes effort, while understating it can leave a subject prepared only for the most obvious form of threat.

[1] Marine Strauss, *Kidnapped Co-Founder of French Crypto Firm Ledger Had His Hand Mutilated*, Reuters (Jan. 24, 2025) (reporting the kidnapping of Ledger co-founder David Balland and his wife, the mutilation of Balland's hand, and a ransom demand payable in cryptocurrency).

[2] Coinbase Global, Inc., Definitive Proxy Statement (Schedule 14A), at 36 (Apr. 24, 2026) (disclosing $7,643,834 in 2025 costs for personal security measures for Brian Armstrong, including residential security, executive protection, family protection, and secure transportation).

© 2026 Collisionless Global Technology Services Inc.

Across the spectrum, risk is a function of perceived reward, perceived accessibility, expected extractability, preparation cost, chance of failure, and consequences of identification. Different actors can view the same person differently because their starting conditions differ. A local opportunist may value immediacy and require little validation. A remote organized group may value scale and invest in reducing uncertainty.

> *The practical task is not to assign one permanent threat label, but to understand which actors could find the available story persuasive, what lowers their cost of action, and what changes make the opportunity less attractive.*

© 2026 Collisionless Global Technology Services Inc.

Target Qualification

Target qualification is the point at which general visibility becomes a particular interest: a judgment that a person may be worth the risk and cost of additional attention. In most cases, the process is identity-first. The starting point is a known person: a founder, executive, developer, investor, trader, collector, conference speaker, or visible community member. Blockchain activity becomes physically relevant when it appears to confirm an existing story about that person. The public identity supplies context; the financial activity supplies apparent validation; business success, counterparties, public statements, lifestyle, and third-party claims add weight.

This is where the distinction between tracing and attribution becomes operationally important. Even a sound attribution does not necessarily establish beneficial ownership, exclusive control, or current access. A wallet may contain business funds, pooled assets, customer property, institutional holdings, shared control, or assets related to a former role. A person may have approved a transaction without owning the funds or once controlled an address that is no longer accessible. In financial investigations, those conclusions require different evidence. A criminal assessment may collapse all of them into a simpler proposition: this person has money and can move it.

The operative variable is therefore perceived wealth, not a defensible net worth calculation. Public discussion of investments or gains, a senior role in a valuable company, an attributable transaction, luxury travel or purchases, a reputation as an early holder, and third-party statements about custody can reinforce one another. The danger is amplified when several sources appear independent even though they repeat the same original claim. Source handling teaches that repetition is not corroboration; ten websites can echo one unsupported wallet label or inflated estimate. A responsible assessment traces the claim to its origin and assigns confidence accordingly. An offender may simply count the echoes.

© 2026 Collisionless Global Technology Services Inc.

Qualification also requires some belief about accessibility and extractability, which should be assessed separately. Accessibility concerns whether the subject or a related person can be contacted, approached, deceived, isolated, or pressured. Extractability concerns the actor's belief that pressure can produce a transfer, credential, approval, ransom payment, device, or cooperation from someone else. A person can be easy to locate and unable to produce value; another may be difficult to reach but surrounded by accessible relatives, staff, assistants, or vendors. Strong custody controls can make actual extractability low while failing to reduce risk if the public story suggests immediate personal control. Publicly explaining the custody design can create a different problem by identifying decision makers or alternate people who matter.

> *Incorrect qualification remains dangerous because accuracy is not a prerequisite for action. The stronger defensive question is not simply whether each claim is true, but whether the available facts support a coherent story that someone might believe.*

© 2026 Collisionless Global Technology Services Inc.

Exposure Accumulates Across Sources

Most dangerous profiles are assembled from ordinary fragments. A professional biography identifies the person. A company page explains the role. An event announcement supplies a date and city. A family account reveals a neighborhood. A public record suggests an address. A wallet association implies value. A photograph confirms a vehicle or familiar setting. A vendor, assistant, or colleague reveals a trusted relationship. Together, these fragments can answer who the subject is, why the subject appears valuable, where the subject may be found, who else is reachable, and whether pressure might produce payment.

The decisive feature is often corroboration. Information from separate sources appears more reliable when details agree. A stale address becomes more credible when a recent family post places the household in the same area. An old wallet association becomes more relevant when later public statements or activity reconnect it to the person. A conference appearance can refresh an otherwise dormant profile by adding current location and timing.

> *The subject may think of these disclosures as belonging to separate areas of life; the outsider does not.*

Separation frequently fails at human seams. Organizations and individuals may create different accounts, wallets, entities, and roles intending to keep them apart, yet reuse a contact point, relationship, device, phrase, image, behavior, or transaction pattern that bridges the separation. Investigations of compartmentalized groups show the same weakness: the architecture can look separate from the inside while ordinary conduct reconnects it from the outside. The question is whether the remaining bridges are strong enough to support a credible inference, not whether formal separation exists on paper.

The household and trusted network expand the exposure surface. Partners, parents, children, assistants, employees, drivers, vendors, and close friends may reveal different parts of the environment, and the easiest person to reach may not be the person who controls assets. Public cases have involved parents abducted because offenders believed their adult child had access to cryptocurrency, as well as families held while one person was pressured to move funds. The consistent pattern is that risk follows perceived leverage. Protecting only the principal can redirect attention toward a more visible or less protected relative, while hardening one communication channel can shift an approach to an assistant.

Time changes the value of information. Addresses become stale, jobs change, devices are replaced, and wealth estimates age, but old information can remain dormant until a new

© 2026 Collisionless Global Technology Services Inc.

disclosure refreshes it. A historical address may become useful when a current post confirms the neighborhood. An old biography may identify a relationship that leads to a current profile. A wallet association thought to be forgotten may regain significance when later behavior appears to confirm continued involvement. Permanence should therefore not be confused with constant usefulness; one new disclosure can restore the value of an old record.

Situational awareness offers a useful way to interpret this accumulation without turning ordinary life into constant suspicion. Investigative work depends on understanding what normal looks like before deciding that a deviation matters. One unusual contact or online interaction may mean little. Several changes across accounts, communications, travel, and the physical environment may justify attention because the pattern has changed. The defensive objective is to recognize combinations that materially improve an outsider's confidence or access, especially when wealth, location, and timing converge in the same window.

© 2026 Collisionless Global Technology Services Inc.

How Information Becomes Useful

Information becomes security-relevant when it changes an actor's options. Wealth signals and professional prominence can support selection. Matching identity details, family connections, transaction associations, and repeated claims can increase confidence that the actor has identified the correct person. Accurate personal or professional facts can add credibility to a false approach because knowledge of a colleague, vendor, event, investment, internal title, or family circumstance may feel like proof of legitimacy. Contact information, event schedules, travel announcements, routines, property records, and household profiles can supply access. Family and business relationships can create leverage. Public statements about self-custody or signing authority can shape the actor's belief about extraction.

These advantages do not require one sophisticated operator. One person may notice a wealth signal, another may know the subject's city or social circle, and someone else may understand how proceeds can be moved. The value of a fact may be that it lowers uncertainty for another participant, validates a rumor, or makes an existing opportunity easier to act upon. Defensive analysis should not assume that an adversary must personally possess every capability from digital research through physical violence and money movement.

> *The most concerning condition is real-time convergence.*

A wallet association or story of wealth may sit online for years without producing a physical opportunity. A location post may be routine and harmless. When apparent wealth, current location, predictable timing, and weak immediate guardianship become visible together, the profile changes. An opportunistic offender already nearby may not need historical depth; an organized actor may use the same information as confirmation that a previously identified opportunity has become accessible. Travel and public appearances deserve particular attention because they can move a person outside familiar protections while advertising where and when that change will occur.

Publicly discoverable facts also weaken informal trust checks. Undercover work repeatedly demonstrated this dynamic. A cold approach begins without an established relationship, but accurate knowledge of the subject’s world could make an unfamiliar person appear informed, connected, and therefore legitimate. Those details did not establish legitimacy; they caused the subject to infer it. The same vulnerability exists when a caller, visitor, message, or request contains accurate information about colleagues, investments, travel, or family. Familiarity can be manufactured when someone knows which details the target treats as signals of trust.

© 2026 Collisionless Global Technology Services Inc.

Consequential decisions should therefore rely on independent verification rather than facts that merely sound private.

Strong cryptography and sound custody architecture remain essential, but they do not eliminate coercion risk. Technical controls protect keys and transactions; they do not prevent pressure against a person. Multi-party approvals, delays, limits, monitoring, and separated authority can reduce actual extractability, create time, and prevent one individual from satisfying an immediate demand. Their value does not depend on public disclosure. Detailed public descriptions can instead reveal the control map and redirect attention to other participants.

Not every exposed fact is material. Most public information never contributes to violence, and an assessment that treats all visibility as equally dangerous becomes alarmist and unmanageable. The disciplined test is whether a fact changes selection, confidence, credibility, access, leverage, timing, or expected extraction. If the connection cannot be explained, the fact may be private or embarrassing without being central to this threat.

© 2026 Collisionless Global Technology Services Inc.

Removal Does Not Resolve Risk

Removal is a necessary tool, but it cannot return an exposed person to an unexposed state. Records have different forms of persistence. Some can be deleted, corrected, suppressed, or de-indexed. Others survive in public filings, archives, screenshots, copied databases, reporting, third-party profiles, breached data, and blockchain history. Even when the original record disappears, the conclusion it created may continue to circulate. The relevant question is what role a record plays in the connected profile and whether other sources continue to provide the same identity, wealth, access, or relationship information.

Historical identity-to-asset links illustrate the limitation. Moving assets to a fresh wallet does not erase a prior public association or the wealth story built around it. Later behavior may also reconnect new activity to the same person. A new wallet, account, email address, or entity can be useful, but technical separation and identity separation are different outcomes. The latter depends on whether subsequent conduct rebuilds the bridge.

This is sometimes dismissed as security through obscurity. The criticism is incomplete. Secrecy should never substitute for sound custody, verification, or physical protection, but there is no defensive value in making discovery, correlation, location, and monetization free, current, and well organized. Reducing visibility raises the actor's acquisition cost, lowers confidence, shortens the useful life of information, and reduces the chance that general interest becomes a specific opportunity.

> *A burglar choosing between two similar homes may avoid the one with motion lights. The lights are not a barrier, but they increase uncertainty and the perceived risk of detection — often enough to redirect an opportunistic offender.*

Privacy and removal services can materially reduce exposure in data broker and search environments, but they cannot control every public record, family account, third-party publication, breach, screenshot, or onchain record. They are most useful when directed at the strongest pathways and combined with changes in ongoing behavior. Removing an address while relatives continue to disclose the residence does little to alter accessibility; removing a wallet label while public interviews reinforce the same ownership claim does little to alter perceived wealth. Counting removals can therefore create false confidence if the profile remains easy to reconstruct.

© 2026 Collisionless Global Technology Services Inc.

The more useful concept is pathway reduction. Information does not have to disappear to become less operationally useful. An old address loses value when it is no longer refreshed or aligned with current routines. A historical wallet association loses value when it cannot be connected confidently to current activity or control. Remediation succeeds when the strongest pathways are weaker, slower, less current, less reliable, or easier to detect. That standard recognizes the permanence of some records without treating permanence as futility.

© 2026 Collisionless Global Technology Services Inc.

Remediation

Remediation should begin with the connected profile rather than isolated accounts or search results. The first task is to understand what an outsider can see, how reliable each fact appears, which facts genuinely corroborate one another, and which combinations materially change the risk. A long inventory is less useful than a clear explanation of the few pathways that make the subject appear valuable, reachable, and capable of producing payment. False but dangerous beliefs should remain part of the analysis when they are credible enough to motivate action.

Priority should be given to reducing real-time convergence. Travel, public appearances, liquidity events, and periods of heightened publicity deserve additional care because they can refresh dormant associations and place the subject outside normal routines. The objective is not withdrawal from public life, but avoiding a complete, current picture at the moment a bad actor can use it. Delayed posting, restrained discussion of holdings and custody, and tighter control over who publishes location or household information can reduce immediacy without requiring silence.

The household and trusted network must be included according to actual role and exposure. Relatives, partners, staff, assistants, vendors, and advisers do not need identical controls or equal access to information, but they need to understand how their accounts, routines, and communications contribute to the larger profile. Trusted decisions should use verification methods that do not depend on publicly knowable facts. Sensitive information about location, custody, response procedures, and authority should not be unnecessarily concentrated in one person or system. The objective is to prevent the easiest person in the network from becoming an alternate path to the principal or the assets.

Existing identity-to-asset associations should be treated as known once they have been made public. Remediation should avoid refreshing them through new statements, screenshots, transaction references, or behavior that recreates attribution. Material changes to custody or asset location require deliberate planning. A rushed transfer intended to create privacy can introduce operational mistakes, tax or legal consequences, loss, new public links, or unjustified confidence that the historical connection has disappeared. There is no universal migration step that safely solves the problem.

Actual extraction friction should be increased wherever the operational context allows it. Separated roles, multiple approvals, transaction limits, delays, independent verification, monitoring, and custody arrangements can reduce the ability of one person to produce immediate value under pressure while creating time for detection and response. These controls should fit genuine business and household needs and should not be described publicly in a way that identifies the people or conditions required to complete a transaction.

© 2026 Collisionless Global Technology Services Inc.

> *The point is to make immediate extraction genuinely difficult while minimizing information that could redirect the threat.*

The human response must be prepared in advance. The moment of pressure is too late to invent authority, communications, or contingencies. Households and organizations should know who can make decisions, how unusual requests are verified, who must be notified, and which relationships already exist with counsel, security, custody providers, and law enforcement. Multi-jurisdictional investigations repeatedly demonstrate that expertise alone is insufficient when handoffs fail. A technically sophisticated plan that nobody can remember or execute under stress is the appearance of control rather than a functioning one. Procedures should be simple enough to understand, practice, and use under stress.

Finally, the profile should be reassessed from the outside. Exposure changes as roles, relationships, vendors, residences, custody arrangements, and public narratives change. Removed information can reappear, while one interview or post can refresh an association that had become stale. Reassessment should ask whether the strongest pathways are now harder to discover, less credible, less current, more difficult to act upon, and less capable of producing value. That is the measure that connects privacy work to actual risk reduction.

© 2026 Collisionless Global Technology Services Inc.

Conclusion

Onchain transparency becomes a physical security concern when it strengthens a story about a real person. The ledger may provide the financial signal, but ordinary public information supplies the identity, relationships, access, timing, and leverage that make the signal actionable. The threat cannot be understood through wallet analysis alone or through a conventional review of personal information alone. It exists in the connections between them.

The threat is also shaped by the actor. Opportunistic criminals may act on proximity and a crude impression of wealth. Insiders can reduce the cost of validation. Small crews can combine partial capabilities. Organized domestic or transnational networks may invest heavily when the expected return is high enough. Their conclusions do not need to be accurate or admissible; they need only to appear persuasive in light of the actor's risk-reward calculation.

The most defensible response is neither panic nor the promise of invisibility. It is a disciplined reduction of linkability, immediacy, confidence, access, and extractability. Historical associations should be assumed to persist, but their usefulness can be reduced. Strong custody controls should be paired with household awareness, independent verification, and a practiced incident response.

> *Success is not the disappearance of every exposed fact. It is a connected profile that is harder to assemble, less convincing when assembled, more difficult to act upon, and less likely to produce value under pressure.*

© 2026 Collisionless Global Technology Services Inc.

VULNERABILITY ASSESSMENT & REMEDIATION

Talk to Collisionless

collisionless.com
contact@collisionless.com

© 2026 Collisionless Global Technology Services Inc.