NICE Actimize

THE KNOBLE™

Report

Human Trafficking Investigative and Response Guide: World Cup 2026

For Major Events, Everyday Life and Financial Institutions

Table of contents

Why This Guide Exists

The Reality

Human trafficking frequently operates within normal-looking environments and routine activities. Financial institutions, service providers and businesses may encounter individuals and transactions that appear ordinary in isolation but form part of a broader pattern when viewed collectively. Exploitation often depends on control, dependency and manipulation rather than visible force, which means indicators are commonly subtle, distributed and role-specific.

Large events can shift how and where signals appear. Sporting tournaments, conventions and similar gatherings temporarily change movement, housing and spending patterns.

During these periods:

- Individuals and groups may move between cities in compressed timeframes
- Short-term lodging, transport and service-related payments may increase
- Late-night and person-to-person transaction volumes may rise
- Temporary or informal work arrangements may expand

While human trafficking knows no boundaries, these events can amplify and alter baseline patterns, making signal recognition dependent on context rather than single data points.

Financial systems often surface indicators early because exploitation typically involves movement and control of funds. Payments connected to lodging, transport, online advertising, third-party transfers or access to earnings may pass through accounts, cards, applications or cash deposits.

Operationally relevant patterns may include:

- Activity inconsistent with known customer profiles or stated business purpose
- Rapid movement of funds following deposits
- Multiple small payments converging on a single recipient
- Third parties appearing to influence or control account use

These financial signals may align with observations from frontline staff or community members. When combined, human observations and data patterns can help form a more complete risk picture.

Who This Guide Is For

Identification and response depend on multiple professional roles observing different parts of the same system.

This guide is designed primarily for financial crime prevention professionals and other roles that may encounter or help identify indicators of exploitation, including:

- AML investigators and analysts
- Fraud teams
- KYC and onboarding teams
- Watchlist and screening teams
- Data, analytics and monitoring teams
- Branch staff and frontline service workers
- Vendors and contractors
- Hotel personnel
- Car rental personnel
- Airline employees
- Victims and targets of human traffickers

These roles often see early signals through customer interactions, transaction activity and monitoring systems.

The Knoble community also includes professionals who encounter trafficking warning signs from other perspectives, including:

- Local, state, federal and international law enforcement
- Government agencies and liaison teams
- Prosecutors, attorneys and legal professionals
- Regulators and supervisory bodies

These stakeholders may not perform the same frontline detection functions described in this guide, but they rely on the quality of observations, documentation, referrals and reporting produced by financial institutions and other reporting entities. Understanding how signals originate and move through institutions supports better coordination, investigation and response.

Professionals may also encounter situations outside formal roles. Awareness gained in professional settings can inform how individuals recognize and safely report concerns in everyday environments.

Each role may see only part of the picture. When signals are recognized, documented and shared through appropriate channels, they contribute to a broader, multi-agency understanding of risk.

Cold State vs Hot State

People learn best in a calm environment but must often act in real time. This difference matters and this guide is written with both in mind.

Cold state refers to periods of training, preparation and analysis. In this state, people can think through patterns, understand signal types and become familiar with escalation paths. This is when awareness is built.

Hot state refers to real-time situations where something appears inconsistent or concerning.

This may include:

- A tense in-person interaction
- An unusual request or transaction
- A customer who appears controlled or fearful
- A system alert requiring immediate attention

In these moments, individuals do not have time to analyze broadly. They rely on simple cues, established procedures and professional judgment.

Hot-state situations may involve safety considerations for customers, staff and others present. Because of this, responses must be measured, non-confrontational and aligned with institutional processes. Acting impulsively, confronting individuals or attempting to resolve situations independently can create risk.

This guide recognizes that individuals may encounter both states. Early sections build awareness of how signals appear. Later sections provide role-specific guidance on how to respond, escalate, document and support investigation in ways that are safe and consistent with professional responsibilities.

Not every unusual situation is trafficking. However, recognizing when something warrants attention — and knowing there is a structured, safe path forward — allows professionals to act appropriately without needing to resolve the situation alone.

Understanding Trafficking

What is Human Trafficking?

Human trafficking involves the exploitation of a person through force, fraud or coercion for labor, services or commercial sex. In the case of minors in commercial sex, proof of force or coercion is not required.

Trafficking can take several forms:

Sex trafficking	Labor trafficking	Benefits trafficking
involves controlling a person and compelling them to engage in commercial sexual activity. This may occur through threats, debt manipulation, emotional control or physical intimidation. Activity may be advertised or arranged through phones, apps or online platforms.	involves exploiting someone's work or services. This can occur in construction, agriculture, hospitality, cleaning, food service, domestic work and other industries. Workers may be controlled through withheld pay, debt, threats of deportation, confiscated documents or isolation.	involves exploiting individuals who receive government or disability benefits. A trafficker may pose as a caregiver, gain control over financial accounts or benefit cards, and use threats or manipulation to take the funds.

Human trafficking is different from smuggling. Smuggling generally involves transporting someone across a border in exchange for payment. Trafficking involves ongoing exploitation and control. A situation that begins as smuggling can become trafficking if the person is later forced, deceived or coerced into labor or commercial sex under threat or to repay debt.

Understanding these forms helps people recognize that trafficking is not limited to one setting or victim profile.

How Trafficking Works

Trafficking relies on control. That control is often psychological, financial or situational rather than a visible force.

Control mechanisms may include:

- Threats of harm to the person or their family
- Debt that can never realistically be repaid
- Confiscation of identification or phones
- Monitoring movements and communications
- Isolation from support networks
- Manipulation of housing, transportation or immigration status

Victims may appear compliant because resistance carries consequences they believe are worse.

Movement of victims can vary. Some individuals are kept in one location, while others are moved between cities, hotels, worksites or events. Movement can increase during large gatherings where demand is higher, and anonymity is easier. This mobility may manifest as travel patterns, address changes or transactions occurring far from a person's stated home location.

Money flow is central to trafficking. Earnings from exploitation may move through:

- Cash deposits
- Person-to-person payment apps
- Wires or ACH transfers
- Prepaid cards
- Third-party accounts
- Payments for lodging, advertising, transportation or "fees"

Why Major Events Increase Exploitation

Large events can change conditions in ways that increase risk.

Demand spikes may occur when large numbers of visitors gather. This can increase demand for both commercial sex and low-wage or temporary labor.

Temporary housing such as hotels and short-term rentals creates environments where people come and go frequently, making it easier for traffickers to operate without drawing attention.

Rapid mobility allows networks to move individuals between cities as events shift locations. Someone may appear in financial or physical activity in one city and then in another shortly after.

Cash and person-to-person payment surges can occur during event periods, especially at night. Short bursts of payment activity from multiple individuals to one recipient, or frequent cash deposits near event venues or hotels, may be part of the financial footprint.

These patterns do not automatically mean trafficking is occurring. However, when multiple indicators appear together, they should prompt heightened awareness, careful observation and timely reporting.

What Humans Can See (Field Observation)

People often notice the first signs of concern through behavior and context rather than documents or data. These observations do not require specialized training. They involve noticing when a situation does not fit what would normally be expected.

No single indicator confirms exploitation. Multiple indicators together, especially when combined with signs of control or fear, should warrant attention.

Behavioral Indicators

Behavior can reveal when someone may be under control or unable to speak freely.

Possible signs include:

- A person who appears to be closely monitored or prevented from speaking for themselves
- Someone who looks fearful, anxious, withdrawn or unusually submissive
- A companion who answers questions directed at another person
- Limited eye contact or visible distress when certain topics arise
- A person who seems unsure of their location, schedule or plans
- Signs of exhaustion, poor health or neglect
- Inconsistent or scripted explanations

These behaviors can appear in many settings — at hotels, transportation hubs, workplaces, stores, restaurants, bars or service counters. The focus is not on how someone looks, but on how they interact and whether they appear to have control over their own decisions.

Situational Indicators

Context matters - some situations may suggest risk when they do not align with the surrounding environment.

Examples include:

- A person being dropped off and picked up repeatedly by different individuals
- Someone who does not have access to their own phone, identification or money
- A worker who does not know their work schedule, pay details or employer information
- Multiple people sharing one room who seem unrelated and have few personal belongings
- An individual who appears new to the area and cannot explain how they arrived
- Someone being pressured to complete a transaction or service quickly

During large events, situations may involve frequent movement between hotels, short stays or late-night activity tied to visitors. These alone do not prove exploitation, but they can change the level of awareness needed when other indicators are present.

Environmental Indicators

Surroundings can provide additional clues.

These may include:

- High turnover of guests in a room or property with little personal luggage
- Excessive security measures for ordinary activity
- Multiple phones, devices or payment cards associated with one individual
- Advertising for services that appear unrelated to the location or business
- Activity concentrated late at night with frequent comings and goings

During major events, the surge in temporary housing and visitor traffic can make it difficult to spot what's unusual, but even a single concerning behavior can signal that something is off. Paying attention to activity that doesn't fit the setting and noticing when unusual patterns continue over time helps surface potential trafficking situations earlier.

How to Safely Ask Questions

If a situation feels concerning, brief and neutral questions can help assess whether someone can respond freely.

Approaches may include:

- Asking open-ended questions that allow the person to answer in their own words
- Speaking directly to the individual rather than only to a companion
- Keeping questions simple and related to the immediate situation

Examples:

- "Is everything okay with your stay?"
- "Do you need any help with your plans today?"
- "Would you like to speak privately?"

If the person cannot answer without looking to someone else, seems afraid or avoids responding, this may indicate limited control. Do not push for details if it increases risk or discomfort.

When Not to Intervene Directly

Personal safety is important. There are times when direct intervention can increase danger for the person involved or for the observer.

Do not attempt to intervene directly when:

- A situation appears to involve immediate threats or violence
- The person seems closely controlled and unable to speak privately
- You are unsure and the setting feels unsafe

In these cases, observation and reporting through appropriate channels is safer than confronting anyone involved.

How to Report as a Member of the Public

If something raises concern:

- Note what was observed, including time, location and descriptions
- Avoid taking photos or recordings if they could create risk
- Contact appropriate resources, such as local authorities or a trafficking hotline
- Provide factual observations rather than assumptions

Reports based on careful observation can help professionals connect information from different sources. Even small details may become important when combined with other reports.

How to Protect Yourself

This section is intended for individuals who may be experiencing exploitation or believe they are being targeted. It focuses on practical safety, maintaining control where possible and accessing help, even in situations involving pressure, fear or manipulation.

You are not expected to solve the situation alone.

Understanding Control and Coercion

Exploitation is often maintained through psychological control, not just physical force. This control can be subtle, persistent and designed to limit a person's ability to think clearly or act independently.

Common techniques include:

Isolation	limiting contact with friends, family or outside support
Dependency creation	controlling access to money, housing, transport or documents
Monitoring	tracking movements, communications or interactions
Rapid pressure	creating urgency so there is no time to think or ask questions
Emotional manipulation	alternating kindness and threat to create confusion and reliance

These techniques are designed to make situations feel inescapable, even when options may still exist.

Threats Against Family and Loved Ones

Human traffickers often rely on fear and coercion to maintain control.

Examples of such threats include:

- "We know where your family is"
- "Your family is being watched"
- "They will be harmed if you do not comply"

These threats are used to create fear and prevent people from seeking help.

What is important to understand:

- In many documented cases, these threats are **not actively being carried out in real time**
- Traffickers often rely on **fear, uncertainty and lack of verification,** rather than actual surveillance
- Maintaining constant control over multiple people in different locations is **logistically difficult and risky**
- The threat is designed to feel **immediate and unquestionable** so that it is not challenged

This does not mean threats should be ignored. They are intended to feel real and can be deeply distressing.

However, understanding the tactic can help create space for safer decision-making.

A Practical Reframe

When threats involve harm to family, they are often used to create fear and maintain control.

In these situations, it is important to understand:

- The statement itself is a **control mechanism**, not proof of current harm
- The goal is to prevent you from contacting others or seeking help
- The situation may not be as controlled as it is being presented

If it is possible to do so safely, even limited verification (such as indirect contact or delayed communication) can help reduce uncertainty.

If You Feel You May Be at Risk

If something feels wrong or controlling, it is important to slow down and focus on your safety.

Steps you can take include:

- Trust your instincts — confusion and pressure are often part of the control
- Avoid sharing additional personal or financial information
- Take small steps to maintain independence where possible
- Create time and space before making decisions when you can

You are allowed to pause, delay or say you need time.

If Someone Is Controlling Your Money or Work

Control over finances is a common method of maintaining influence.

If possible:

- Keep access to some funds separate from others
- Be aware of where money is being sent or received
- Notice if someone insists on controlling all earnings or transactions
- Recognize patterns where you are asked to transfer money quickly or repeatedly

These patterns can be important if you later seek help.

If You Are Being Moved or Asked to Travel

Movement can be used to reduce familiarity and increase dependency.

If possible:

- Keep track of locations, addresses or names of places
- Note travel routes or cities, even if only mentally
- Pay attention to how frequently plans change without explanation
- Look for opportunities to maintain awareness of your surroundings

Small details can become useful later.

If You Need to Communicate Safely

Communication may be limited or monitored.

If possible:

- Use moments of privacy to reach out to someone you trust
- Share simple, clear information such as location or situation
- Avoid drawing attention if communication is being watched
- Use indirect or low-risk communication methods where needed

You do not need to explain everything at once.

If You Want to Seek Help

You are not required to confront anyone directly.

Options may include:

- Contacting a trafficking hotline or emergency service
- Speaking with a staff member, coworker or service provider
- Using online reporting tools where available
- Reaching out to someone you trust

If there is immediate danger, emergency services should be contacted.

If You Are Unsure What to Do

Uncertainty is common in controlled situations.

You can:

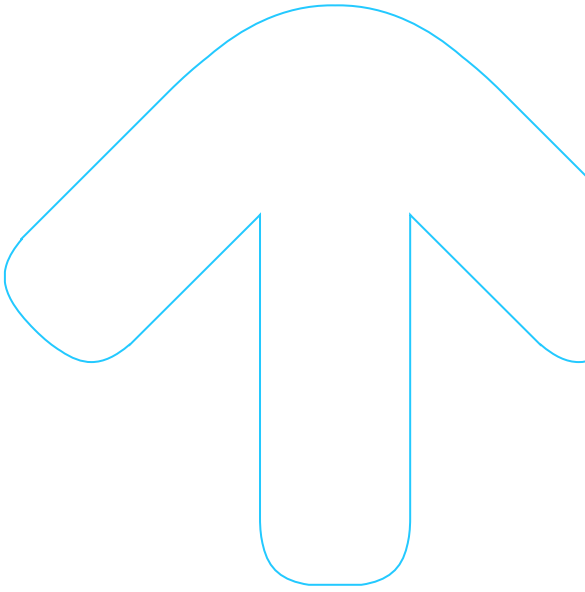
- Focus on maintaining safety rather than solving everything at once
- Take small steps that do not increase risk
- Look for opportunities to create distance, time or communication
- Remember that support services are designed to help without requiring full details immediately

A Practical Reminder

Control often depends on making a situation feel absolute and immediate. It rarely is.

Even in highly controlled situations, small actions — noticing, remembering, delaying or reaching out — can create options over time.

You do not need to prove what is happening to seek help.



What Financial Institutions Can See (Financial Signals)

Financial activity often reflects exploitation before it becomes visible elsewhere. While individuals may only see one interaction, financial institutions can observe patterns over time, across locations and across multiple counterparties. These patterns do not prove trafficking on their own, but they can reveal risk when viewed together.

Why Banks See Trafficking Early

Exploitation typically involves control over money. Traffickers may direct how earnings are received, where funds are sent and how expenses are paid.

Because of this:

- Accounts may show activity that does not match the person's profile
- Payments may cluster around certain times, locations or events
- Funds may move quickly through accounts with little personal spending
- Multiple unrelated people may transact with the same account

These signals can appear in deposit, withdrawal, card, transfer or app-based payment activity. When frontline observations and financial patterns align, the overall risk picture becomes clearer.

Technology and Data Sources

Financial institutions use various tools to detect patterns that may relate to exploitation.

These include:

Transaction monitoring, which identifies unusual activity based on behavior, amount, timing or deviation from expected patterns

Link analysis, which shows relationships between accounts, devices, contact details and counterparties

Consortium intelligence, which allows institutions to identify patterns that may span multiple organizations

These tools support pattern recognition, but human review remains important. Analysts, investigators and frontline staff contribute context that systems alone cannot provide.

Role-Based Detection in Financial Institutions

Different roles encounter different signals. No single team sees the full picture. When observations from people, transactions and data are combined, risk becomes easier to identify.

Branch and Frontline Staff

What to observe during in-person interactions:

- A customer who appears controlled or monitored by someone nearby
- Someone who does not seem to understand their own account activity
- A person pressured to complete a transaction quickly
- Limited access to identification, phone or personal information
- Repeated visits for deposits or withdrawals tied to similar amounts
- Individuals who seem unfamiliar with the local area or their own address

Conversation techniques:

- Use calm, neutral questions related to the transaction
- Speak directly to the individual when possible
- Offer opportunities for private conversation
- Observe whether the person can answer freely or looks to someone else

The goal is not to investigate, but to determine whether the person appears to have control over their situation.

Reporting Steps

If observed indicators raise concern about potential exploitation, it is important to report in line with established procedures.

In these cases:

- Follow internal escalation procedures
- Document what was observed, not assumptions
- Include dates, times, behaviors and transaction details
- Do not confront or accuse

Fraud Teams

Transaction Behaviors Resembling Coercion

- Sudden changes in account usage patterns
- Transactions inconsistent with the customer's profile
- Frequent small transfers to or from multiple individuals
- Unusual device or access patterns

Authorized Push Payments (APP) Fraud Overlap

Some victims of trafficking may be coerced into sending or receiving funds under direction.

Fraud signals and trafficking signals can intersect when:

- A person appears to be acting under pressure
- Transactions benefit a third party rather than the account holder
- Funds move quickly after receipt

Collaboration between fraud and AML teams helps determine context.

AML Investigators

Typologies and Flow of Funds

- Multiple senders to one account
- Cash deposits followed by rapid transfers
- Payments tied to lodging, transportation or advertising
- Accounts with high activity but little personal expense use

Network Development

- Identify shared contact information or devices
- Map relationships between related accounts
- Look for patterns repeated across customers
- Patterns that show centralized control over earnings can be relevant.

KYC and Onboarding

Identity Anomalies

- Documents that appear inconsistent with the person presenting them
- Customers unsure of their own contact details
- Third parties completing applications on someone's behalf

Shared Data Patterns

- Multiple customers using the same address, phone number or email
- Repeated use of identical employment information
- Connections to high-risk industries with little detail

These indicators may suggest vulnerability or external control.

Watchlist and Screening

Adverse Media Signals

- Reports linking individuals or businesses to exploitation
- Online advertisements or public postings suggesting commercial services

Open Source Intelligence (OSINT) Connections

- Shared contact information across online platforms
- Public listings that match financial or identity data

Open-source information can provide context when other signals exist.

Analytics and Data Science

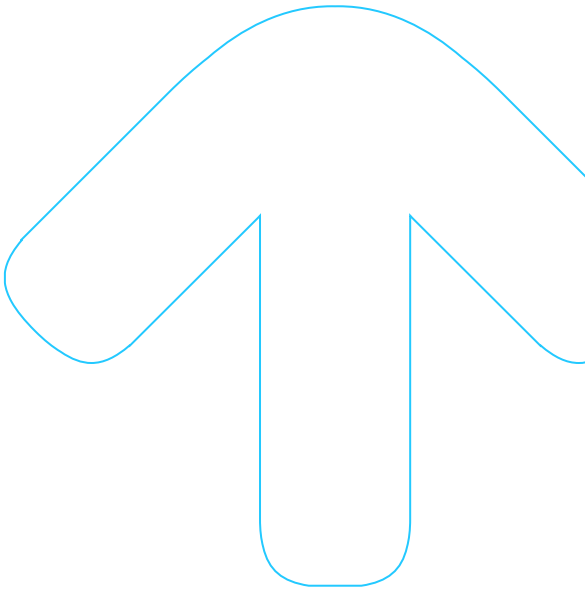
Pattern Recognition

- Identify clusters of similar transactions across customers
- Detect deviations from normal behavioral baselines
- Monitor velocity and repetition of small-value payments

Event Surge Modeling

- Track temporary spikes in activity near event locations
- Monitor short-term increases in person-to-person payments
- Analyze shifts in geographic patterns during major gatherings

Analytical models support detection, but human review provides interpretation.



Event-Specific Typologies

Large events can change how exploitation appears. Activity may intensify over short periods, shift locations quickly and involve temporary arrangements that do not resemble long-term patterns. Recognizing these dynamics helps place observations and financial signals in context.

Traveling Exploitation Networks

Some networks move individuals between cities as events shift locations or as demand changes.

Indicators may include:

- Individuals appearing in one city for a short period, then reappearing elsewhere
- Financial activity tied to travel, lodging or transportation across multiple locations
- Similar transaction patterns repeating as events move
- Limited personal belongings or unstable housing situations

For frontline observers, this may look like frequent check-ins and check-outs or repeated short stays. In financial data, this may appear as activity in different geographic areas within a compressed timeframe.

Micro-Payment Aggregation

Exploitation can involve many small payments rather than a few large ones.

Patterns may include:

- Repeated low-value payments from multiple individuals to one recipient
- Activity concentrated during evenings or overnight
- Payments that appear unrelated to the stated purpose of the account
- Rapid movement of funds after receipt

These patterns can resemble other behaviors, but when combined with mobility, control indicators or contextual signals, they may warrant closer review.

Hotel and Venue-Based Activity

Temporary lodging and event venues can become focal points during large gatherings.

Possible signals include:

- Frequent short stays linked to the same individuals or payment sources
- High levels of traffic to and from a room without typical travel patterns
- Payments for rooms, rides or services that do not align with normal visitor behavior
- Cash or card activity clustered near hotels, arenas or entertainment districts

These environments can provide anonymity and frequent turnover, which can make patterns harder to detect without awareness.

Labor Exploitation During Events

Events often require temporary labor in construction, cleaning, food service and support roles. This can increase vulnerability for workers.

Indicators may include:

- Workers who appear unsure of pay arrangements or employer details
- Groups transported together with limited control over schedules
- Third parties managing wages, housing or identification documents
- Financial activity showing earnings quickly transferred to another account

Labor exploitation may not be visible in public-facing roles but can still appear in financial or identity patterns.

Cross-City Pattern Repetition

Exploitation networks may repeat similar methods as they move.

This can include:

- Similar transaction structures appearing in different cities
- Shared contact information, devices or payment channels across locations
- Recurring clusters of activity tied to event timelines
- Consistent use of certain service providers, lodging types or transport patterns

When observations from different locations show comparable signals, it can suggest coordinated activity rather than isolated incidents.

Response Framework

Recognizing indicators is only the first step. How people respond can affect safety, investigations and outcomes. The goal is to document concerns and route information to the right place without increasing risk.

If You Are a Member of the Public

You are not expected to investigate. Your role is observation and reporting.

If something feels concerning:

- Focus on what you directly saw or heard
- Note time, location and descriptions of people or vehicles if safe to do so
- Avoid confrontation or attempts to "rescue" someone
- Do not promise help you cannot provide

Contact appropriate resources such as a trafficking hotline or local authorities. Provide factual observations rather than conclusions. Small details from multiple people can later form a clearer picture.

If You Are Frontline Staff

Your interaction may be brief, but your observation can be important.

When concerns arise:

- Continue normal customer service while maintaining awareness
- Ask neutral, situational questions if appropriate
- Do not accuse or alert a potential trafficker
- Follow internal procedures to escalate concerns

Document behaviors, statements and transaction details. Even if the activity seems low value, repeated reports can reveal patterns over time.

If You Are an Analyst

You may be reviewing alerts, referrals or patterns.

When evaluating activity:

- Look at behavior over time, not just one transaction
- Consider customer profile, stated occupation and normal activity
- Identify links between accounts, devices or contact details
- Review geographic movement and timing

If patterns align with known indicators, escalate according to internal processes. Collaboration between fraud, AML and KYC teams can provide additional context.

If There Is Immediate Danger

If someone appears to be in immediate physical danger:

- Prioritize safety
- Contact emergency services
- Avoid direct intervention that could escalate the situation

Clear threats, violence or medical emergencies require immediate action rather than internal reporting alone.

Internal Escalation vs Law Enforcement

Not every concern requires direct law enforcement contact by individuals.

In most cases:

- Members of the public report to appropriate hotlines or authorities
- Frontline staff report internally through established channels
- Analysts escalate through compliance or investigation teams

Organizations determine when and how to involve law enforcement based on policies and legal requirements. Information shared internally allows trained teams to assess risk, protect individuals and support appropriate reporting.

Investigation Playbook

Once concerns are escalated, structured review helps determine whether isolated signals reflect a broader pattern. The goal is to move from single observations to a clear understanding of behavior, relationships and risk.

Confirming Indicators

One signal alone rarely provides enough context.

Investigators and reviewers should:

- Look for repeated behaviors over time
- Compare activity to the customer's stated profile
- Identify whether patterns appear across multiple products or channels
- Consider whether behavioral, geographic and financial signals align

Consistency across different data points strengthens the assessment.

Mapping the Network

Exploitation often involves multiple individuals or facilitators. Network development helps reveal structure.

This may include:

- Identifying shared contact details, devices or addresses
- Reviewing common counterparties or payment recipients
- Linking accounts that transact frequently with one another
- Looking for central accounts that receive funds from many individuals

Network mapping can show whether activity is independent or coordinated.

Linking Financial Activity to Movement

Mobility patterns can be reflected in transactions.

Reviewers may look for:

- Card use, deposits or withdrawals in different cities over short periods
- Activity that shifts in line with travel or event schedules
- Travel-related expenses tied to accounts receiving clustered payments
- Repeated location changes that mirror other accounts in the network

When financial movement aligns with physical movement patterns, risk assessment becomes more informed.

Documentation Best Practices

Clear documentation supports effective review and reporting.

Good practices include:

- Recording facts, not assumptions
- Including dates, times, transaction details and observed behaviors
- Noting why activity differs from expected patterns
- Referencing related accounts or connections

Consistent documentation allows others to follow the reasoning behind decisions.

Writing Strong Internal Referrals

Internal referrals help teams share concerns across functions.

Effective referrals:

- Summarize the key indicators observed
- Describe how patterns developed over time
- Highlight links to other accounts or customers
- Include relevant supporting data

Clear referrals support a timely and coordinated review.

Writing Effective Suspicious Activity Reports (SARs)

When required, reporting should focus on behavior and patterns.

Helpful elements include:

- A concise description of suspicious activity
- Explanation of how transactions and behaviors connect
- Identification of related parties and accounts
- Notation of geographic movement or timing relevant to risk

The goal is to provide a clear picture of activity so that external reviewers can understand why concern exists.

Information Sharing and Legal Framework

Information sharing helps connect signals that may appear unrelated when viewed in isolation. At the same time, privacy and confidentiality rules exist to protect individuals and investigations. Understanding these boundaries supports responsible detection and reporting.

SAR Confidentiality

SARs are a key reporting mechanism for financial institutions.

Important principles include:

- The existence of a SAR, or the decision to file one, must not be disclosed to the customer or unauthorized parties
- Internal discussion should be limited to those with a need to know
- Documentation and communications should avoid language that reveals SAR filing status

Maintaining confidentiality protects investigations and prevents tipping off individuals who may be involved in criminal activity.

314(b) Information Sharing

Certain legal frameworks allow financial institutions to share information with one another for the purpose of identifying and reporting potential criminal activity.

Under these provisions:

- Institutions can share information related to possible money laundering or other financial crimes
- Participation requires registration and adherence to regulatory guidelines
- Shared information should be relevant, factual and properly documented

Information sharing can help identify broader networks when different institutions each see part of the picture.

Privacy Considerations

Detection efforts must balance awareness with respect for privacy.

Good practices include:

- Sharing only information that is necessary for a legitimate purpose
- Limiting access to sensitive data to authorized personnel
- Documenting the reason information was accessed or shared
- Following internal policies and applicable laws

Protecting privacy supports trust and ensures that detection and response efforts remain responsible and compliant.

Quick Reference (Hot State Tools)

When situations unfold quickly, people rely on memory shortcuts rather than detailed training. Simple cues help convert awareness into action.

One-Page Visual Red Flag Sheet

If something feels concerning, look for combinations of behavioral, situational and environmental cues.

Behavioral Cues

- Signs of being controlled, coached or unable to speak freely
- Fearful, withdrawn or overly watchful behavior
- Someone else holding identification, phone or documents

Situational Cues

- Frequent short stays or visits
- Unusual movement of people at late hours
- Limited personal belongings for the length of stay

Environmental Cues

- High traffic to a room or location
- Signs of multiple occupants but little visible personal activity
- Locations near major events, transport hubs or temporary housing

One indicator alone may mean little. Patterns matter.

Financial Red Flag Checklist

Financial activity can reveal patterns associated with potential exploitation.

When reviewing transactions or account behavior, look for:

- Many small payments from different people to one account
- Rapid movement of funds after deposits
- Activity inconsistent with the customer's profile
- Shared contact details, devices or addresses across customers
- Card or ATM use across distant locations in short timeframes
- Third parties appearing to control account use
- Multiple movie rentals from hotel room
- Liquor store purchase patterns
- Multiple hotel charges for the same day (many rooms scenario)

Financial signals become more meaningful when paired with behavioral or geographic indicators.

Event Surge Checklist

Large events can temporarily shift transaction and movement patterns.

During these periods, pay attention to:

- Sudden spikes in person-to-person payments
- Increased late-night transaction activity
- Short-term lodging, travel and transport expenses
- Accounts active in an event city for a brief period, then move

These patterns may reflect normal event activity, but combinations of signals may warrant review.

Reporting Decision Tree

See Something Concerning?

Immediate danger or medical emergency?

Contact emergency services.

Public observer or service worker?

Document what you saw and report to the appropriate hotlines or internal supervisors.

Frontline staff in an organization?

Follow internal escalation procedures. Record facts and observations.

Analyst or investigator?

Review patterns, link related data and escalate according to policy.

When in doubt, document and report through the appropriate channel. Multiple small reports can connect to form a larger picture.

Continuous Improvement

Detection and response do not end with one report or one investigation. Exploitation methods change, and awareness improves when information is shared and lessons are applied.

Why Reporting Matters

Many individual observations may seem minor on their own.

However:

- Small details from different people can connect over time
- Repeated reporting helps identify patterns
- Early reporting may help prevent further harm
- Financial data combined with frontline observations can reveal larger structures

Consistent reporting supports both immediate response and long-term prevention.

Feedback Loops

Learning improves when information flows between roles and organizations.

Effective feedback may include:

- Sharing typologies and trends with frontline staff
- Updating monitoring rules based on confirmed cases
- Informing analysts about new behavioral or geographic patterns
- Providing awareness training that reflects recent events

When teams understand how past signals contributed to outcomes, future detection becomes stronger.

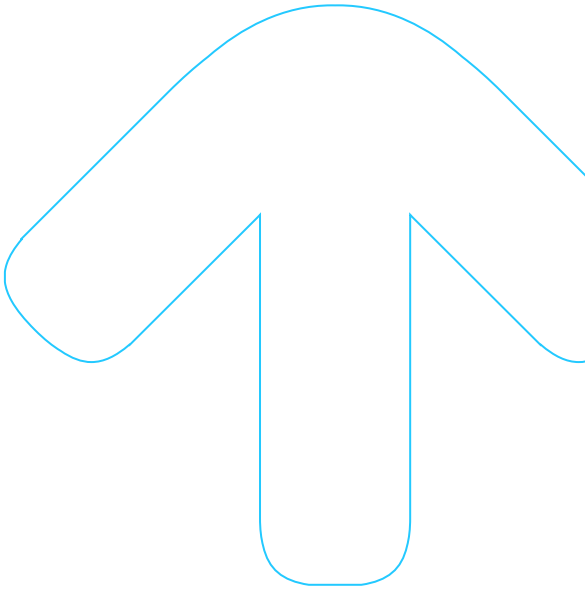
Evolving Trafficking Methods

Those involved in exploitation adapt to controls and awareness.

Changes may include:

- Shifting to new payment methods or platforms
- Using smaller transaction amounts to avoid detection
- Moving between cities or events more quickly
- Adjusting recruitment or control tactics

Ongoing awareness helps ensure that detection efforts keep pace with changing behavior.



Conclusion

Human trafficking often remains hidden not because signs are absent, but because they are dispersed across people, places and systems. No single observation or data point tells the full story. Awareness across communities, frontline roles and financial systems helps bring those pieces together.

“If You See Something, Say Something”

Trusting your observations matters.

You do not need proof. You do not need to know exactly what is happening. Reporting what you saw, heard or noticed allows trained teams to connect information over time. Many cases begin with small, routine observations that seem minor when viewed in isolation.

Document what you observed. Follow the appropriate reporting path. Your role is to share information, not to investigate.

Collective Responsibility

Prevention and detection rely on many different roles working together.

Different roles may observe different indicators:

- Members of the public may notice behavior or situations
- Frontline staff may observe interactions in real time
- Analysts may see financial or data patterns
- Organizations may connect signals across locations

When these perspectives are combined, risks become easier to identify and respond to. Each person’s contribution helps strengthen overall awareness and response.

Appendix

Glossary

These terms, where applicable, are explained below to support understanding by both the public and financial professionals.

Account Monitoring: Tools and processes that review transactions and patterns to detect unusual activity.

Behavioral Indicator: Observable actions of a person that may suggest limited control over their situation, such as inability to speak freely or deferring answers to another.

Entity Linkage: Analysis showing connections between accounts, devices or contact details.

Financial Pattern: A recurring structure in transactions (e.g., small payments from many senders) that may suggest exploitation when combined with other signals.

Geographic Signal: Financial or physical activity that appears inconsistent with a person's stated residence or normal patterns.

Link Analysis: A method of identifying relationships between data points, such as shared devices or contact information.

Micro-Payment Aggregation: Many small-value payments converging on a single recipient within a short time period.

Network Mapping: The process of visualizing relationships between people, accounts and transactions.

Person-to-Person (P2P) Payments: Direct transfers between individuals through apps or platforms.

Situational Indicator: The context around a person's activity that may suggest risk, such as repeated short stays in lodging during large events.

Transaction Monitoring: Technology that detects unusual financial activity based on predefined rules and patterns.

Traveling Exploitation Network: A group that moves individuals between locations, often syncing with events or demand spikes.

Resources and URLs

- **National Human Trafficking Hotline** – Connects people to help and allows reporting of suspected trafficking. 1-888-373-7888 (phone) | Text BeFree (233733) | https://humantraffickinghotline.org/en
- **Transportation Security Administration – Report Trafficking** – Tip reporting and support resources. https://www.transportation.gov/stop-human-trafficking
- **U.S. Department of Homeland Security's Blue Campaign** – Public awareness and educational resources. https://www.dhs.gov/blue-campaign
- **U.S. Department of Justice – Human Trafficking Resources** – Victim assistance information and official guidance. https://www.justice.gov/humantrafficking/resources

- **Polaris (National Hotline Operator)** – Training, data, and anti-trafficking resources. https://polarisproject.org
- **International Coordination (ICAT)** – United Nations anti-trafficking information exchange. https://icat.un.org
- **Stop the Traffik** – Global awareness, intelligence, and prevention resources. https://en.wikipedia.org/wiki/Stop_the_Traffik
- **Global Alliance Against Traffic in Women (GAATW)** – International NGO network focused on systemic change. http://gaatw.org

Hotline Numbers

United States & International (U.S.-based reporting):

- **National Human Trafficking Hotline:** 1-888-373-7888 (24/7 in >200 languages) | **Text 233733 (BeFree)**
- **Blue Campaign / DHS Tip Line:** 1-866-347-2423 (24/7)
- **Emergency (if someone is in immediate danger):** 911 (U.S.)

Canada:

- **Cybertip.ca (Child exploitation reporting):** https://www.cybertip.ca/ (Includes trafficking of children via online exploitation)

(For World Cup–specific local hotlines – these can vary by host city/country. When final host cities are known, include relevant municipal human trafficking or emergency numbers.)

Sample Reporting Forms and Mechanisms

- **National Human Trafficking Hotline – Online Tip Form**
  Submit confidential reports online with structured fields for observations, dates, locations, and contact details (optional). https://humantraffickinghotline.org/en/report-trafficking
- **DHS Blue Campaign Reporting Resources**
  Guidance on contacting Federal tip lines, including information to include in reports.
  https://www.dhs.gov/blue-campaign/report-human-trafficking
- **ICE HSI Tip Line**
  Call or web form for reporting broader suspicious activity, including trafficking.
  Call: 1-866-347-2423

(Organizations and institutions should use internal referral forms tailored to AML, fraud or compliance reporting. These forms should prompt for: date/time, observed behavior, transaction details, geographic locations and related identifiers.)

NICE Actimize | THE KNOBLE™

Know more. Risk less.

info@niceactimize.com
niceactimize.com/blog
@NICE_actimize
/company/actimize
NICEactimize

About NICE Actimize

As a global leader in artificial intelligence, platform services, and cloud solutions, NICE Actimize excels in preventing fraud, detecting financial crime, and supporting regulatory compliance. Over 1,000 organizations across more than 70 countries trust NICE Actimize to protect their institutions and safeguard assets throughout the entire customer lifecycle. With NICE Actimize, customers gain deeper insights and mitigate risks. Learn more at www.niceactimize.com