CONVERGENCE

Child Sexual Exploitation and Abuse

Detecting and Disrupting Child Sexual Exploitation and Abuse (CSEA) Across Financial Systems

SUMMARY REPORT • OCTOBER 1, 2025

Event Overview

The day began with a Women in Risk breakfast, focusing on empathy, allyship, and the resilience and know-how required to address cases involving Child Sexual Exploitation and Abuse (CSEA). The conversation set a collaborative tone that carried into the Convergence sessions. We closed together with Child Rescue Coalition's "Blankets & Bear Hugs" activity, assembling care kits for children encountered during law enforcement investigations, purposefully bookending the day with heart and action.

To underscore why this work matters, a letter from a veteran detective was read aloud, describing a six-year-old girl who was frightened during a search warrant. Her experience changed when she was handed a Blankets & Bear Hugs kit. She never let go of the bear. That human impact framed the day's mission: convert risk signals and intelligence into protection, and protection into hope.

The Convergence working sessions focused on four CSEA risk detection categories: Grooming, Travel/ Sex Tourism, Livestreaming (long-distance abuse), and CSAM Production, and blended transactional behaviors with open-source and contextual indicators to improve accuracy, speed, and scale.

Key Take-aways

- We opened with a Women in Risk (WIRE) Breakfast and closed with Child Rescue Coalition's "Blankets & Bear Hugs," bookending the day with empathy and action.
- A law enforcement letter shared during the closing underscored the real-world impact: care kits can transform a traumatized child's experience during law enforcement operations.
- Panel takeaway: entity context + behavioral detection must work together; neither alone is sufficient for CSEA typologies.
- Working sessions focused on Grooming, Travel/ Sex Tourism, Livestreaming, and CSAM Production, pairing transactions with OSINT, device/IP, occupation/access, and geolocation.
- Next steps: productize new indicators in risk cards, refine SAR impact paths, maintain the engineer and investigator build loops, sustain team resilience, and continue offering giving-back programs like Blankets & Bear Hugs at future events.

©2025 Quantifind, Inc.

WOMEN IN RISK PANEL SUMMARY

Breaking Barriers, Building Better Outcomes

Moderator: Marianne Trefz (Quantifind)

Key Insights

- Technology and Identity Context: Modern CSEA financing patterns are characterized by small-value and high-velocity transactions across multiple services. Effective detection requires the fusion of entity and identity contexts with behavioral analytics, two capabilities that must operate in tandem.
- Co-Building Typologies: Investigators and technologists co-develop typologies in tight iteration loops, rather than handing off requirements, yielding sharper signals and lower noise.
- Empowering Analysts: Self-serve data tools enable analysts to adjust thresholds, pull and manipulate data, and move faster as patterns evolve; CRC datasets provide invaluable starting points.
- SARs that Move Cases: Close the filing/outcome gap by prioritizing narrative quality and including IP/device IDs, wallet IDs, travel metadata, and role/access clues; build direct law enforcement pathways in priority jurisdictions.
- Strength for the Battle: Normalize resilience practices (limits, compartmentalization, intentional breaks). Grow allyship and mentoring; diverse perspectives expand investigative range.
- Advice to the Next Generation: Become a go-to SME; embrace lateral moves and cross-sector experience; learn the foundations of casework and internal data landscapes to lead transformationally.

Convergence Event Working Group Highlights (by Typology)

Notes by: Marianne Trefz (Quantifind), Tyler Strickland (Quantifind)

A. Grooming Typology

Grooming indicators discussed by participants highlighted overlapping financial and behavioral signals. Common cases included adults making purchases of gifts or payments to minors across peer-to-peer apps and gaming platforms. Examples included CashApp, Zelle, Roblox, and OnlyFans credits found on minors' accounts. 'Big girl incentives'—branded luxury gifts, such as those from Sephora or concert tickets—were cited as tactics to build trust. Other signs involved low-value hotel bookings near home addresses and inconsistent spending patterns, suggesting concealment.

- Purchase & incentive patterns: gaming ecosystems (e.g., Roblox/Robux), P2P (e.g., Cash App, Zelle), branded incentives (e.g., Lululemon, Sephora, concert tickets), and OnlyFans credits appearing on a minor-linked account.
- Local hotel transactions near a customer's residence, layered with frequency and geolocation, offer practical starting signals; hotel quality is informative when misaligned with the wealth profile.
- Context is critical: differentiate parents vs. non-familial adults; incorporate occupation/access-to-children (e.g., teachers, coaches, volunteers) to elevate risk where access exists.

Key Actions for Institutions

- Cross-reference transactions with declared dependents and customer occupations
- Flag adults with access-to-children professions for enhanced review
- Use counterparty surname matching to identify non-familial links
- Apply contextual scoring for hotel and travel proximity to home
- Integrate behavioral clustering and social context in AML typologies

©2025 Quantifind, Inc.

CONVERGENCE EVENT WORKING GROUP HIGHLIGHTS (CONTINUED)

B. Travel / Sex Tourism Signals

Travel-related indicators often reveal mismatched lifestyle behaviors. High-net-worth individuals booking low-grade hotels in high-risk regions such as the Philippines, Thailand, Uganda, or Eastern Europe were discussed. Patterns included large cash withdrawals, avoiding credit cards to prevent visibility to spouses, and repeat visits to rural locations. Participants recommended integrating OSINT, hotel data, and remittance records to identify concealed travel associated with exploitation.

Signals to Watch For

- High cash withdrawals near airports or foreign ATMs
- Budget hotel stays inconsistent with the income profile
- Wires to NGOs or small charities in high-risk countries
- Recurring trips to remote or low-tourism regions
- Avoidance of credit card payments or transparent records

Key Actions for Institutions

- Use OSINT and map validation to confirm hotel locations
- Leverage 314(b) exchanges to link travel and wire data
- Integrate NGO screening to flag shell or front organizations
- Correlate cash withdrawals and travel bookings for anomalies
- Prioritize geographic risk scoring with behavioral overlays

C. Livestreaming Signals (Long-Distance Abuse)

Livestreaming exploitation involves repeated small-value payments to obscure streaming or chat-enabled platforms. Participants highlighted the rise of in-house payment applications and similar tools that embed messaging features, requiring concurrent monitoring of transactions and chat data. Institutions underutilize device IDs and IP tracking, which could reveal gender or linguistic mismatches between senders and receivers. CRC shared a 20-factor risk model emphasizing ethnolinguistic variance, sex-offender registry overlaps, and multi-wallet associations.

Signals to Watch For

- Microtransactions to unrecognized streaming or hosting platforms
- Professional camera or lighting equipment purchases without clear business reason
- Linked wallets or repeated use of same IP/ device IDs across accounts
- Chat-enabled payments through new fintech platforms
- Gender or cultural mismatches between senders and recipients

Key Actions for Institutions

- Correlate streaming payments with device/IP identifiers and account linkages
- Apply natural language processing to detect illicit coded communication
- Strengthen KYC and transaction monitoring for streaming creators
- Monitor crypto and fintech integrations for emerging chat-payment typologies
- Partner with NGOs to update detection models for evolving services

CONVERGENCE EVENT WORKING GROUP HIGHLIGHTS (CONTINUED)

D. CSAM Production Typology

The production of CSAM increasingly involves legitimate-looking platforms, such as OnlyFans or Patreon, where offenders disguise their content as adult entertainment. Investigators described creators funneling income through multiple sites while portraying minors. Other red flags included large camera purchases, coded messages, and geographic, or language shifts upon account reopening. The group also discussed AI-generated CSAM as a growing threat requiring new detection frameworks.

Signals to Watch For

- Multiple inbound payments from adult-content platforms to one account
- Large purchases of video production equipment without a declared business purpose
- Coded emojis or hidden messages in payment memos
- Frequent login/IP changes or language switches across sessions
- Inconsistency between customer profile and transactional behavior

Key Actions for Institutions

- Flag accounts receiving funds from multiple adult-content sources
- Combine hardware purchase data with platform payouts for risk correlation
- Incorporate AI-based tools to identify synthetic CSAM patterns
- Expand SAR narratives with device IDs, IP logs, and crypto traces
- Collaborate globally on AI-CSAM standards with UNODC and CRC

Institutions Represented
(Women in Risk and Convergence)

Financial Institutions:	Ally Bank; U.S. Bank; Bank of America; Wells Fargo; Truist; Synovus; City National Bank; Goldman Sachs; TIAA; Fifth Third.
Payments / FinTech:	Western Union
Crypto Exchange:	OKX
Multilaterals / NGOs:	United Nations / UNODC; Polaris; Child Rescue Coalition (CRC); Sentinel Foundation
Tech / Platforms:	Cisco Systems

Final Thoughts and Next Steps

- Productize new CSEA risk indicators by integrating OSINT and contextual signals (occupation, proximity, device/IP, and travel granularity) into risk cards.
- Enhance SAR impact by elevating narratives with digital identifiers, travel metadata, and role/access clues; establish direct LE pathways (domestic & foreign).
- Engineer the feedback loop: keep technologists and investigators co-building; maintain self-serve data tooling at the edge.
- Normalize resilience practices and expand allyship/mentoring initiatives through Women in Risk (WIRE) and partner communities.
- Carry the activism forward: continue Blankets & Bear Hugs at future convenings – reminding teams who we serve.

Join Women in Risk Elevated (WIRE) to connect, collaborate, and rise together as leaders redefining the future of financial crime detection and mitigation. This community exists to elevate women's voices, champion allyship, and translate our collective expertise into meaningful action.

Join The Convergence Network to collaborate across institutions, share intelligence, and co-create new solutions that enable us to fight financial crime with accuracy, speed, and scale.