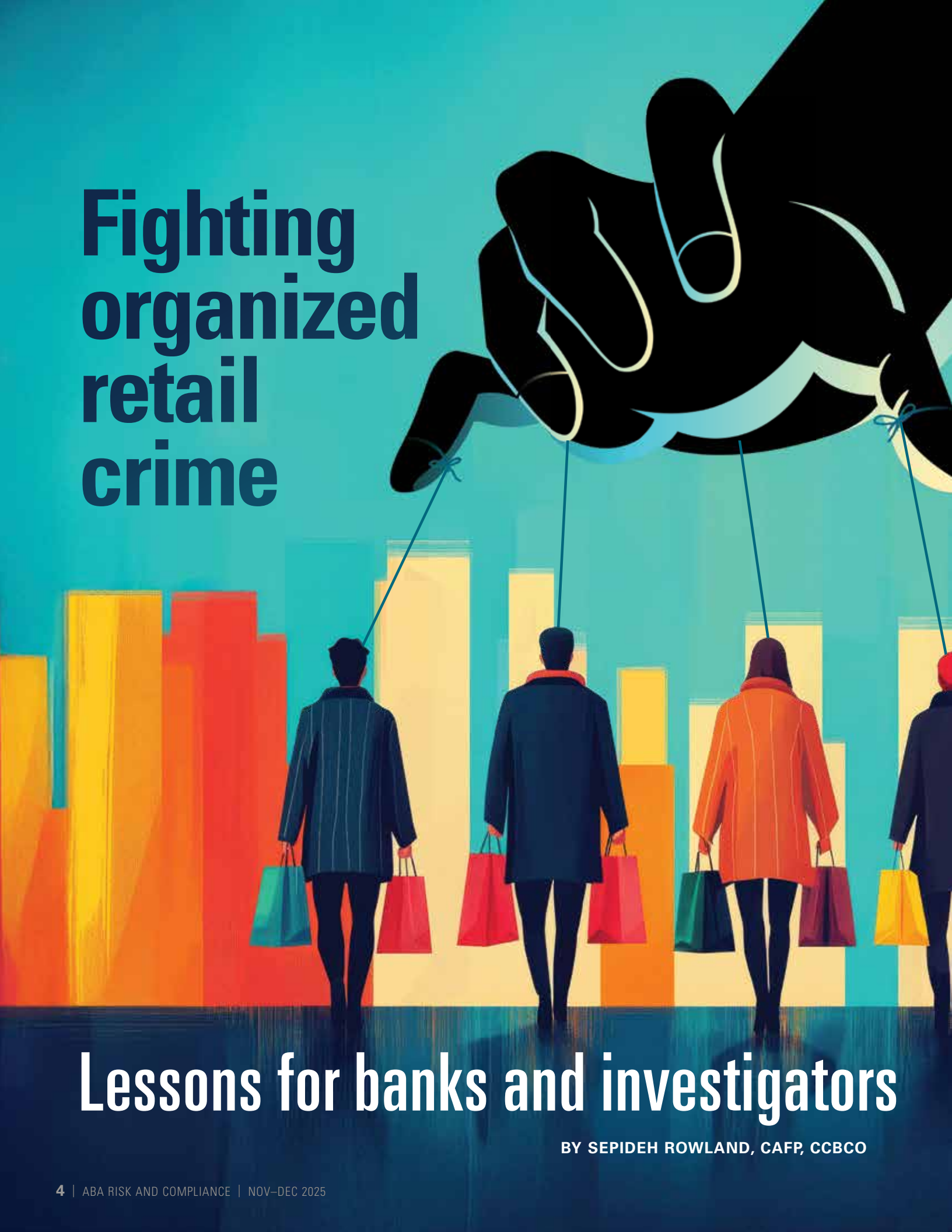
Fighting organized retail crime



Lessons for banks and investigators

BY SEPIDEH ROWLAND, CAFP, CCBCO

Insights from Raul Aguilar, former deputy assistant director for the Countering Transnational Organized Crime, Financial and Fraud Division of Homeland Security

FROM THE OUTSIDE, Michelle Mack appeared to live an enviable life. She and her husband owned a vineyard estate in Southern California complete with a chapel they rented out for weddings, while raising their children in the quiet community of Bonsall. But behind the scenes, Mack was orchestrating a sprawling organized retail crime (ORC) ring involving at least a dozen women who shoplifted from stores across the country — including more than 230 Ulta Beauty locations. Prosecutors say she provided the target locations, paid travel expenses, and then resold the stolen cosmetics on Amazon under a company registered to a local post office box as "Online Makeup Store." In all, more than $8 million in merchandise moved through her network before the Macks were arrested in December 2023, and over $300,000 in goods were found during a raid on their home. Her case is a striking example of how ORC is not petty theft; it's a lucrative, organized business model, often hiding in plain sight.[1]

The national threat and the federal response

Michelle Mack's case is not an anomaly; it reflects a growing and dangerous trend. Across the country, organized retail crime (ORC) has escalated into a national threat involving professional criminal groups that steal large quantities of goods from retail stores with the intent to resell them through online marketplaces, brick-and-mortar fronts, and even international distribution networks. Far from isolated shoplifting incidents, these operations often involve smash-and-grab thefts, cargo hijackings, and coordinated fraud. According to the federal agencies, ORC is now a multibillion-dollar criminal enterprise that not only impacts commerce and consumer confidence, but also poses risks to public safety and national economic security.

To address the increasingly complex and transnational nature of these crimes, the federal agencies are backing legislation like the Combating Organized Retail Crime Act of 2025,[2] which would establish a national Organized Retail and Supply Chain Crime Coordination Center. This proposed center would support cross-jurisdictional investigations by improving information sharing and resource allocation among federal, state, and local law enforcement. In addition to legislative efforts, the federal agencies actively coordinates investigations, prosecutes ORC offenders, and promotes partnerships between law enforcement and the private sector. Public awareness is also a key element in how the government is addressing this strategy. The agency encourages consumers to report suspicious online listings and highlights the broader societal impact of ORC: the closure of neighborhood stores, increased prices, job losses, and threats to health and safety from improperly stored or counterfeit goods.

Homeland Security Investigations' Operation Boiling Point is a national initiative targeting ORC networks through coordinated enforcement, leveraging public-private collaboration. Since its launch, the operation has resulted in dozens of arrests, indictments, and multimillion-dollar asset seizures, driven in part by information-sharing partnerships with retailers and FIs. These cases highlight the growing recognition of the banking sector's critical role in identifying suspicious financial activity and supporting law enforcement in dismantling ORC operations from the inside out.

STOCK.ADOBE.COM / WARUNTHORN / RUDALL30

A Conversation with Raul Aguilar: Inside organized retail crime

To better understand the evolving threat landscape of organized retail crime and how FIs can play a more proactive role in disrupting it, we turned to Raul Aguilar,[3] one of the nation's leading voices in transnational criminal investigations. Raul recently joined Auror, a retail crime intelligence platform, as senior director of law enforcement partnerships, after a distinguished career at Homeland Security Investigations (HSI), where he served as deputy assistant director for the Countering Transnational Organized Crime, Financial and Fraud Division. At HSI, Raul helped shape the federal response to investigate complex criminal networks, including those fueled by ORC-related activity.

In my conversation with Raul, we discuss how organized retail crime networks operate, the red flags financial institutions should be watching for, and the critical role of public-private partnerships in turning intelligence into disruption.

"Organized retail crime isn't a fringe issue — it's a multibillion-dollar criminal enterprise."

Raul, to start, can you help us define organized retail crime and explain why it's more than just shoplifting?

Organized retail crime, sometimes called organized retail theft, refers to coordinated, large-scale theft operations — not petty shoplifting. These are structured criminal enterprises involving two or more individuals who steal merchandise from retailers, commit fraud, and then convert those goods into cash, often by reselling them online or through other illicit channels. The money is then funneled back into the organization to fund additional criminal activity.

We're talking about professional crews with clearly defined roles — some members are responsible for the theft, while others handle logistics, sales, and proceed laundering. This involves anything from cargo theft to targeting specific retailers, where they know exactly what products to steal and how much profit they can make from them. It's a repeatable, profitable business model, and the proceeds are reinvested back into the network to sustain and grow the operation.

Just how widespread is organized retail crime today, and what should FIs understand about its scale?

It's a massive and growing problem. Coming out of COVID, the explosion of e-commerce and the ease of creating anonymous seller accounts has made it even more lucrative. Organized retail crime isn't a fringe issue — it's a multibillion-dollar criminal enterprise.

According to recent reports from RILA and the National Retail Federation, nearly $70 billion in goods are stolen from retailers annually.[4] Even if just a fraction of those items are resold online or through other channels, that still amounts to hundreds of millions — if not billions — of dollars in illicit proceeds. These funds often support broader transnational criminal networks involved in everything from drug trafficking to fraud. FIs need to be aware that they may be unknowingly facilitating these transactions.

Can you talk more broadly about the kinds of products that are typically targeted in these crimes? Is it mostly consumer goods, or is the scope wider?

The most commonly targeted items include pharmaceuticals, home improvement supplies, groceries, household goods, electronics, and health and beauty products — things that are easy to grab and resell. We've seen a lot of focus on cosmetics, as you mentioned, and also a big uptick in the auto space, especially catalytic converter thefts. In fact, the FBI and HSI have made some significant takedowns related to those thefts in recent years.

Clothing and apparel are also major targets. Due to safety or violence concerns, many stores have "do not engage" policies for staff, and if the value of goods stolen stays under the felony threshold, organized crews know they can get in and out quickly without much consequence. They run in, grab what they want, and run out — sometimes hitting multiple locations in a single day.

From a consumer standpoint, though — why should people care? It's easy to assume big box retailers can absorb the loss.

It's a fair question, but the impact is bigger than most people realize. First, there's the safety concern. The people working in these stores — our family members, neighbors, and friends — are often the ones at risk when these thefts happen. Innocent bystanders can be injured or traumatized.

Then there's the economic side. Estimates suggest retail theft adds about $500 a year in costs for the average family.[5] That's because stores have to raise prices to offset their losses. And when theft becomes too costly, stores close — especially pharmacies — which reduces access to essential services and jobs in the community. So this isn't just about merchandise walking out the door. It's organized crime with ripple effects across entire neighborhoods.

STOCK.ADOBE.COM / MAHSIN

Let's talk about what happens after the theft. Where does the merchandise go, and how has online selling — especially since the pandemic — changed that?

Once the items are stolen, usually by individuals we call "boosters," they're passed up the chain to middlemen known as fences.[6] These fences are the key players who resell the goods through a variety of channels. Some run brick-and-mortar stores or pawn shops. Others operate out of warehouses or flea markets. In California, there are even pop-up houses where crews sell high-end goods and they know exactly what to target and how much they can profit.

Then, of course, there's the digital side — e-commerce websites where the anonymity makes it easier to offload stolen merchandise. Some fencing operations work with organized groups that build full-scale online selling pipelines. In some cases, particularly with things like iPhones, the stolen goods are even exported overseas, fueling an international smuggling network.

As a banker, how might this activity show up in transactional monitoring? What red flags should I be looking for?

It starts with knowing your customer — really knowing them. That means strong onboarding and vetting processes. Look for red flags like structured payments, multiple accounts using the same addresses, shell companies, or even stock photos on business profiles.

From a compliance standpoint, SARs should be written with enough detail to be useful for investigators. Granularity matters. And beyond the data, community engagement is also critical. Banks often work with law enforcement around drug or human trafficking; we need that same kind of partnership for organized retail crime.

States such as Maryland, Virginia, Michigan, and California have strong retail associations that are now inviting bankers and FIs to the table. That's a great way to learn how criminal funds move through the system and how banks can adjust their monitoring accordingly.

"Banks are not bystanders. They are essential players in disrupting these networks."

You and I have often discussed the power of public-private partnerships. When banks and law enforcement collaborate, they can turn intelligence into real disruption. What's the value of those partnerships in tackling organized retail crime?

Consistent communication is critical, whether it's through webinars, online forums, or in-person meetings. Back when we launched Operation Boiling Point at Homeland Security, we saw firsthand that real impact only happens when communities come together. We had retailers, law enforcement, and prosecutors involved, but what was missing early on was the financial sector. Once we brought banks into our quarterly threat briefings, we really started to see momentum.

What does organized retail crime actually look like on the ground? How much money is involved, and what are some of the fraud typologies connected to it?

It varies, but the scale is massive. Take gift card fraud as just one example. It's grown into a $100 million fraud industry in just the past few years. That's why ongoing communication with community partners is so important. These conversations lead to larger conferences and breakout sessions where we can dig deeper into specific trends and threats.

And I want to highlight the role of academia, too. Universities are increasingly engaged in studying transnational organized crime and illicit financial flows. Institutions like the University of Florida's Loss Prevention Research Council[7] are leading research into loss prevention, including how money moves through Romanian crews and South American theft groups. To make a real impact, it's going to take this kind of collective effort from banks, law enforcement, retailers, and researchers.

Let's take a closer look at Operation Boiling Point. Can you walk us through how some of these cases unfold, such as the Michelle Mack case?

Absolutely. One of the biggest challenges in identifying ORC is that it's highly decentralized and scattered across jurisdictions. Ground-level law enforcement might respond to a theft at a store, but without a structured and shared reporting system, those individual events often look isolated. That's where we miss the larger network.

That's where technology comes in. For example, now retailers can submit detailed, structured reports to platforms — whether the incident involves theft, return fraud, or gift card fraud. That information can then be shared directly with law enforcement, helping connect the dots. From there, the case can move upstream, often in collaboration with prosecutors to determine whether it should be pursued at the state or federal level. And in many cases, those incidents are found to have links to broader criminal networks.

Let me give you two real-world examples. The first is a case out of Boston tied to an Organized Crime Drug Enforcement Task Force investigation. This wasn't just your typical retail theft crew. The criminal network involved was also engaged in drug trafficking, weapons offenses, human trafficking, and even COVID relief fraud. A huge part of their revenue was coming from organized retail crime — several criminal business lines they were running simultaneously. These kinds of hybrid operations are becoming more common as ORC is being used to fuel and fund other forms of transnational organized crime. This is where FIs become critical. Once you know what to look for, you start to see how the money moves.

Now let's take the Michelle Mack case in California. She's been referred to as the "beauty queen" behind a sophisticated ORC operation. She had a network of boosters — people assigned to steal specific items off detailed shopping lists. They primarily targeted high-end cosmetic stores. This wasn't random theft. They knew exactly what SKUs had the highest resale value. These individuals treated it like a day job: get up, steal what was on the list, bring it back to Mack, and she would handle the resale.

She sold the stolen goods online through a storefront called "Online Makeup Store." Some buyers likely didn't know the items were stolen, but others probably did. Over time, that storefront pushed more than $8 million in stolen goods. With the proceeds, Mack purchased a $2.75 million home, and law enforcement traced hundreds of thousands — possibly up to a million dollars — through her bank accounts.

And where do banks fit in when it comes to advancing investigations and prosecutions?

So what could a bank have seen? That's where the lessons are. Were there structured deposits being made just below reporting thresholds? Multiple accounts tied to the same mailing address or post office box? Did anyone question how a business selling makeup was suddenly generating millions of dollars in volume? Were stock photos or vague business descriptions being used to mask the true nature of the business?

Banks need to be on the lookout for these kinds of anomalies. This is where knowing your customer [KYC] and enhanced due diligence really matter. You want compliance teams that go beyond basic box-checking. You want them writing SARs [Suspicious Activity Reports] that contain detail — granular descriptions of what's happening and why it raises red flags.

This is also where community engagement and public-private partnerships come in. Banks need to connect with their local law enforcement agencies, join retail crime coalitions, and stay looped into discussions around financial flows and fraud typologies.

In the Mack case, restitution was eventually ordered. But imagine how much damage could've been prevented if the red flags were spotted earlier. The point is: banks are not bystanders. They are essential players in disrupting these networks. But they have to know what to look for, and they have to ask the right questions.

Taking the Michelle Mack case as an example, this type of activity isn't usually uncovered through a SAR, correct?

That's a great point, Sepideh. Most organized retail crime investigations like the Michelle Mack case, don't start with a SAR. They usually begin with an alert from a retailer or a suspicious pattern picked up by law enforcement. But once an investigation is underway, SARs become critical for seeing the bigger picture.

Once a retailer alerts law enforcement and an investigation begins, at what point do you go back and look for a SAR?

That typically happens as law enforcement begins mapping out the financial aspect of the case. SARs provide important threads that can link seemingly unrelated transactions, accounts, or entities. The challenge is that the activity often looks small in isolation — one deposit, one transaction, one account. But when patterns emerge across multiple institutions or geographies, those SARs become powerful tools. That's why it's essential for banks to train teams to recognize ORC red flags, just as they do for drug or human trafficking.

And how much do you rely on the information a bank provides, especially when the activity may look small or isolated at first?

We rely on it heavily. That's why it's essential for banks to train their teams to recognize organized retail crime red flags — just as they do for drug or human trafficking. ORC should be part of compliance training, onboarding, customer due diligence, and transaction monitoring. The small stuff such as gift card fraud, EBT abuse, low-level stolen goods, adds up fast. But if banks are only looking for high-value transfers, they're going to miss it.

The challenge, however, is what happens after the SAR is filed. Law enforcement faces hurdles ingesting that data in a usable format and connecting it to other pieces. That's especially tough with ORC, which is scattered across jurisdictions. In places like Southern California, for instance, gift card fraud, EBT abuse, and stolen goods are moving through dozens of financial institutions daily. Without a centralized hub, those onesies and twosies are hard to pinpoint with a holistic view.

That's why banks need clear protocols and training to help staff identify red flags, whether using existing reports or building their own internal resources like red flag one-pagers. The challenge for law enforcement isn't just in the content of the SAR itself but how it's received, processed, and analyzed. Turning those reports into actionable intelligence requires the right technology to identify patterns and connect the dots across cases.

So I think the community effort is really important, with banks engaged in their own cities and communities, raising awareness about these threats and focusing on specific red flags. These could come from the reports we've written, or banks might identify their own and create go-to resources, like one-pagers, to help their teams spot suspicious activity.

We recently saw a major win in California with the takedown of a large skimming operation involving Romanian and South American theft crews. The case resulted in around $8 million in losses and more than 50 arrests. It worked because state, local, and federal agencies collaborated, shared data, and had the tools to track patterns across financial systems.

This kind of success underscores the power of public-private collaboration. Banks that stay active in their communities and remain alert to ORC typologies can play a vital role in disrupting these networks before the damage spreads.

I believe inviting law enforcement into your bank to train your teams on the real cases they're actively investigating is one of the most effective ways to build public-private collaboration. It helps bankers connect transaction patterns to real-world criminal activity.

Exactly. And beyond training, banks should take full advantage of the 314(b) process to share information with other institutions. If you're seeing something like skimming or gift card fraud in your area, chances are other banks nearby are seeing it too. And if law enforcement has made an arrest tied to your region, it's a good opportunity to reach out to your AUSAs or bank liaison officers and ask, "Could we be affected?"

This isn't about investigating every case in depth. It's about spotting major ones and recognizing patterns that may affect your institution. Just as

repeat offenders often hit multiple retailers, the same tactics are likely used across banks. If one bank is exploited, others may be too. Criminals use familiar tactics: structuring small deposits, falsifying employment, fake addresses. The more we talk to each other, the more we can piece together and disrupt the larger network.

How can we help FIs look beyond ORC red flags to recognize broader criminal activity, like human or labor trafficking?

The key word is "organized." These aren't isolated thefts — they're coordinated, multi-layered operations.

Take labor trafficking, for example. We've had documented cases in Houston where undocumented individuals, often from Central America, were trafficked specifically to steal. They were handed shopping lists and sent out daily to hit multiple stores, often targeting pharmacies. The stolen goods were funneled back up the chain, sold by fences, and distributed through online or physical storefronts.

Then there's the illicit massage business typology tied to Chinese money laundering. We've seen hundreds of millions of dollars flow through shell businesses and payment platforms. Often, those fronts involve trafficked Chinese nationals working under horrific conditions. Banks might see transaction activity tied to massage businesses, but behind the scenes it's tied to sex trafficking, labor exploitation, and broader money laundering.

Other cases — like the Northeast gang linked to organized retail theft, COVID relief fraud, narcotics, and weapons trafficking — show how deeply interconnected these crimes are. These aren't just return frauds or stolen goods; we've seen boxes of rocks returned to stores for refunds after stealing iPhones from multiple locations. They even exploit store rewards systems.

The creativity and coordination of these networks mean banks must look beyond a single red flag. One retail SAR could be part of a much larger, more dangerous operation.

How are criminal organizations using crypto to facilitate the sale or purchase of stolen goods?

Cryptocurrency has become a powerful tool for criminal networks, who use it to hide profits by moving funds across coins, wallets, and exchanges. It's a growing abuse vector, and savvy criminals know how to exploit it.

What's missing is a coordinated law enforcement and industry response. Law enforcement needs better tools and training to trace crypto, especially at fiat conversion points. Partnerships with international experts and blockchain analytics firms are key — as seen in takedowns like Silk Road and AlphaBay.

But organized retail crime is often left out of these crypto discussions. I work closely with the National Retail Federation and the Retail Industry Leaders Association, and there's limited focus on crypto's role in this space, or on how banks can detect related activity. That's a blind spot we need to address. Criminals are already using crypto to their advantage, and banks should be part of the solution.

"These crimes directly impact our neighborhoods. When stores close or employees don't feel safe, that hurts everyone."

As we wrap up, what's your call to action for financial institutions? Where can banks lean in more, and how can the industry help close some of the remaining gaps?

I think the momentum is there — we just need banks to step up and create their own best practices. Each bank should look inward and ask: What are we missing in our training and education efforts? How can we build webinars or internal sessions that not only inform our own teams but also support law enforcement and retail investigators?

And I have to give credit to those retail investigators. They're working long hours across the country, chasing organized crews and digging into cases. They're a vital part of this ecosystem, and we need to bring them into the conversation. If they understand the banking perspective such as how financial patterns are tracked, and what a suspicious deposit looks like, they'll be better equipped to provide law enforcement with actionable intel that can loop back to FIs.

That feedback loop hasn't really been formalized yet, but it should be. We should see ORC investigators speaking at financial crime conferences, especially in the fraud space, which naturally bridges banks and retail security. That's where I think real progress can be made — when both sides learn each other's playbook and start building solutions together.

These crimes directly impact our neighborhoods. When stores close or employees don't feel safe, that hurts everyone. Banks are the connective tissue and the backbone of local economies. Banks are uniquely positioned to spot red flags early, support public safety, and help preserve prosperity in the places they serve. ■

ABOUT THE AUTHOR

SEPIDEH ROWLAND, CAFP, CCBCO, is the co-chair of the Editorial Advisory Board for *ABA Risk and Compliance* and a senior compliance executive with extensive leadership experience. She has served in key roles such as chief compliance officer, and BSA/AML and sanctions officer, at several of the financial industry's most respected institutions, community banks, and money services businesses. Sepideh was honored with the 2023 American Bankers Association Distinguished Service Award for Financial Crimes in recognition of her outstanding career and contributions to the banking industry. Connect with her at **linkedin.com/in/sepidehrowland**.

Endnotes

1. https://oag.ca.gov/news/press-releases/attorney-general-bonta-secures-prison-sentence-against-organized-retail-crime
2. https://www.congress.gov/bill/119th-congress/house-bill/2853
3. https://www.auror.co/the-intel/raul-aguilar-joins-auror
4. https://www.ice.gov/about-ice/hsi/news/hsi-insider/op-boiling-point
5. https://www.icsc.com/uploads/default/ICSC_ORC_Brief_Fall_2023.pdf
6. https://www.justice.gov/archives/jm/criminal-resource-manual-1343-criminal-redistribution-stolen-property-fencing
7. https://lpresearch.org/

RESOURCES

Criminal Justice Data: Organized Retail Crime
www.congress.gov/crs-product/R48061

Article: Organized Retail Crime
nrf.com/advocacy/policy-issues/organized-retail-crime