

How Consortium Data Is Changing Commercial Fraud Defense

Rich insights layered into secure payments processes can deliver efficiency, accuracy, and precision that strengthen prevention efforts.

By Dalit Amitai and Jen O’Conner



Fraud in commercial banking is evolving faster than most financial institutions’ ability to fight it. Banks increasingly are searching for ways to strengthen their fraud prevention tactics and are turning to consortium data, or shared intelligence across multiple institutions, as a powerful tool.

Consortium data provides insights, signals, and behavioral patterns no single institution could produce on its own. When multiple banks encounter the same beneficiary and one has already confirmed it as fraudulent, that shared awareness can turn a borderline alert into a critical one. With those benefits in mind, the message from banks is clear: richer, broader intelligence is highly valuable when layered into secure payments processes.

The commercial fraud landscape is especially nuanced. Larger transaction sizes, more users involved, and higher operational complexity all contribute to increased risk. Consortium data helps address this by offering visibility in three core areas:

- Portfolio-level patterns inside a bank's own book
- Consortium-level insights from peer institutions
- Industry-level trends shaping the broader fraud environment

Together, these layers build a stronger, more trustworthy fraud detection strategy.

“The commercial fraud landscape is especially nuanced. Larger transaction sizes, more users involved, and higher operational complexity all contribute to increased risk.”

What Banks Want to Know About Consortium Options

One of the most common questions among financial institutions is whether all consortiums are created equal. The short answer is “no.” A consortium limited to transaction-level data or dependent solely on self-reported fraud provides only a fraction of the value banks expect.

The strongest consortium models share several non negotiable characteristics:

- They must be additive, offering meaningful incremental intelligence
- They must be easy to access, without requiring new projects or heavy integrations
- They must integrate directly into the bank’s existing risk platform, so investigators see insights as part of their normal workflow

The importance of this last point cannot be overstated. When consortium data is natively embedded into a risk-mitigation platform, banks avoid costly implementations and immediately benefit from enriched signals.



From an operational perspective, this is transformative. Today, without integrated signals, investigators often need to pivot across multiple systems, consult colleagues, or manually re enter payment information just to determine whether a new or unknown beneficiary is risky. Integrated consortium data eliminates that friction, reduces the possibility of manual error, and preserves data integrity.

Beyond efficiency, integration makes the consortium a true component of the analytics engine. The platform can automatically check consortium insights during the risk scoring process. If the payment is confirmed as low risk, the system may never surface the alert at all, saving investigators significant time and reducing noise.

Why a Commercial Payments Focused Consortium Matters

Many banks initially underestimate how different commercial fraud is from retail fraud. For any bank serving business clients, a consortium focused specifically on commercial payments is essential.

Because commercial payments fraud often flows through complex cash management ecosystems, having a fraud organization embedded within a payments company enables unique visibility. This includes in network activity across global cash management platforms, revealing nuanced business payment behaviors and emerging fraud patterns that would be invisible to an individual institution.

When this visibility is paired with sophisticated analytics and native fraud models, it produces meaningful, measurable value in fraud detection and false positive reduction. Recent modeling across 10 banks showed the potential to reduce false positives by up to 20%. This reduction is driven by the consortium's ability to recognize indicators of known, legitimate payees and safe account behavior across participating institutions, signals that are invisible to any single bank evaluating a new or unfamiliar payee in isolation.

For an investigator working 100 alerts per day, that reduction would lower the volume to 80 without sacrificing safety. For teams of five or six investigators, this is equivalent to gaining the capacity of an additional full time employee, completely through increased efficiency. Importantly, that recovered capacity can be redeployed to lower alert thresholds and responsibly expand risk appetite, enabling

stronger fraud prevention and earlier intervention without increasing operational burden.

Where the Industry Goes Next

The appetite for broader visibility and stronger, shared intelligence is clear. As organizations look for ways to reduce friction, streamline operations, and strengthen defenses, consortium data has become a natural next step.

What matters most to banks as financial crime becomes increasingly organized, coordinated and network-driven is the need for better insights, less noise, and fraud defense tools that match the network nature of modern commercial payments risk.

Consortium data directly addresses this reality. By pooling intelligence across participants, it enables stronger detection, fewer unnecessary alerts, and a more resilient payments ecosystem, one where no institution has to fight a networked threat alone.

-Dalit Amitai is Head of Product, Risk Solutions and Jen O'Connor is a Sales Account Executive at Bottomline.



Protect Payments. Preserve Trust. Stay Compliant.

Fraud is evolving and so are expectations. Payments Fraud Defense helps reduce risk, streamline investigations, and meet NACHA requirements, so fraud doesn't become loss and compliance is built in.

Build confidence in every transaction.

**[CLICK TO STAY NACHA-COMPLIANT
AND LEARN MORE.](#)**

