

# Fighting Financial Crime Within Your Institution — And Beyond

The Power of Consortium Analytics



The threat of financial crime is growing across the globe. The recent push towards real-time payments along with the emergence of cryptocurrency has accelerated the adoption of electronic transactions.

Criminals have seized the opportunity, adapting money laundering and fraud typologies to take advantage of the speed and convenience of real-time payments and the pseudo-anonymity offered by cryptocurrency. Meanwhile, bad actors have remained focused on traditional payment rails such as wire and ACH, furthering their fraud and money laundering activities across these channels. With faster payments, an increasing number of transaction channels, a global footprint, and interconnected criminal activity, financial institutions face significant challenges in the fight against financial crime.

Transnational organized crime, which includes a broad range of criminal activities such as drug and weapons trafficking, human trafficking, and money laundering, is growing<sup>1</sup> while crimes against consumers increases.<sup>2</sup> Unconstrained by privacy rules, government regulations, technology, and geographic boundaries, criminals readily share and sell personally identifiable information (PII). Financial institutions have been slow to respond and losses are escalating — they need a solution to keep pace with growing global financial crime.

### The Global Impact of Financial Crime

The impact of the world's financial crime epidemic is immense. In 2023, globally, banks faced \$442 billion in projected losses from payments, check, and credit card fraud. Meanwhile, consumer scams touched every region, amounting to \$43.6 billion in estimated losses.<sup>3</sup>

Authorized Push Payment (APP) fraud has quickly become a preferred method of attack across the globe,<sup>4</sup> yet liability continues to shift. While fraud victims expect their financial institutions to protect them from loss, who is ultimately responsible for losses remains undecided.

In 2023  
**\$442B**  
lost globally to  
payments, check  
and credit card fraud

Up  
**\$43.6B**  
lost worldwide  
to consumer scams

1 United Nations Office on Drugs & Crime, Transnational Organized Crime: The Globalized Illegal Economy, N.D., <https://www.unodc.org/toc/en/crimes/organized-crime.html>

2 Federal Trade Commission, Who Experiences Scams? A Story for All Ages, 2022, <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages>

3 Nasdaq, 2024 Global Financial Crime Report, 2024, <https://www.nasdaq.com/global-financial-crime-report>

4 Payment Systems Regulator, PSR confirms new requirements for APP fraud reimbursement, 2023, <https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/>

In 2024, the United Kingdom introduced regulations requiring financial institutions to reimburse victims of APP scams. This regulatory change has made the UK the first jurisdiction in the world to introduce legislation for APP scam reimbursement, bringing with it a need for a more focused response to help mitigate fraud, while maintaining the customer experience.<sup>5</sup>

Consumers look to their financial institutions to protect them from financial crime loss; however, within the U.S. there is less debate around liability and U.S. customers currently bear the burden of loss. As a potential liability shift for consumer-related payment fraud gains momentum within regulatory spheres in the U.S.,<sup>6</sup> financial institutions face increased pressure to reduce fraud losses, effectively manage operational costs, minimize customer friction, and mitigate reputational risks.

### **A Unified Approach with Collective Intelligence**

While criminals execute fraud and money laundering activities across networks spanning multiple transaction channels, multiple financial institutions, and multiple jurisdictions, many institutions' approaches to anti-financial crime are fragmented.

Too often, financial institutions rely on their own siloed data sets and outdated technology such as on-premises, rules-based transaction monitoring systems and disconnected point solutions — approaches that provide only a limited view of criminal activity. A single financial institution investigating financial crime alone is limited to just one side of the story. To truly understand fraud and money laundering networks, financial institutions must look beyond their own four walls to break down silos and utilize innovative solutions that keep pace with evolving financial crimes.

Consortium data and analytics offer a crucial step change to break down siloes, unify institutions, and enable the industry to decisively disrupt financial crime.

---

5 Authorised Push Payment Reimbursement Models, Jonathan Frost & Nasdaq Verafin, 2024, <https://verafin.com/resource/shifting-liability-authorised-push-payment-reimbursement-models/>

6 United States Senate, Letter to Consumer Financial Protection Bureau, 2022, [https://www.reed.senate.gov/imo/media/doc/letter\\_to\\_cfpb\\_re\\_instant\\_payment\\_services\\_07-20-2022.pdf](https://www.reed.senate.gov/imo/media/doc/letter_to_cfpb_re_instant_payment_services_07-20-2022.pdf)

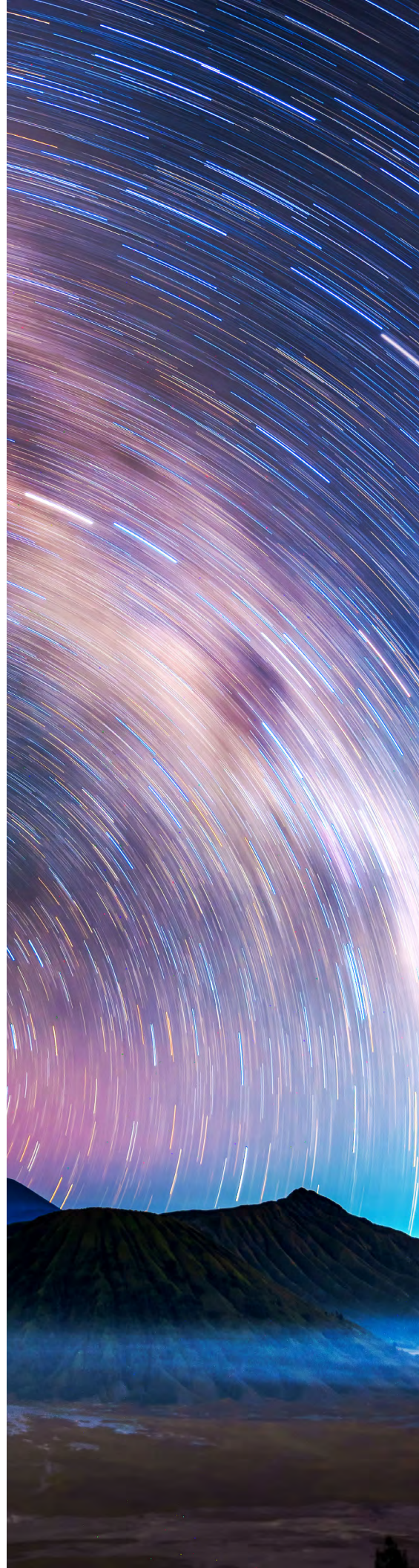
## Consortium Data and Analytics

Cloud-based consortium data enables institutions to identify patterns of criminal activity, evolving trends, and financial crime risks more effectively across institutions. To truly disrupt financial crime, financial institutions need visibility into the originator and the beneficiary of a transaction, and consortium analytics provides this insight beyond the confines of a single institution. With a full breadth of anonymized and standardized data, comprehensive consortium analytics can be developed to detect and disrupt fraud, money laundering, and predicate crimes.

In a cloud-based consortium network, each financial institution contributes data into a standardized data model for consortium-level analysis, enabling greater insight into customers and the counterparties they interact with. Large consortium-based data sets also allow anti-financial crime technologies to profile counterparties beyond the network — layers of rich demographic and transactional information in the consortium data set are leveraged to profile accounts and entities outside the consortium to identify low-and high-risk counterparties.

Consortium analytics provide a unique and essential contribution to managing and preventing financial crime. When criminals collaborate, sharing malicious practices and evading detection, consortium analytics and counterparty analysis offer financial institutions an approach to benefit from collective insights across a consortium network, without sharing PII. By analyzing consortium-based data from multiple financial institutions — in the hundreds or thousands, technology providers can develop anti-financial crime solutions that enable fraud detection and AML/CFT consortium analytics, providing institutions with greater insights into risk.

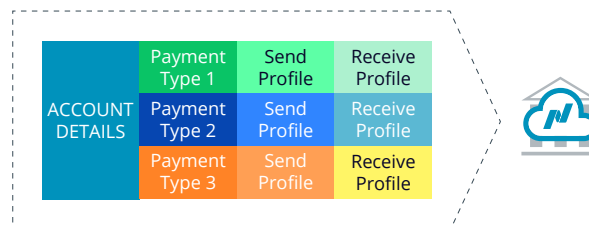
With this collective intelligence approach, consortium data and analytics offer a more accurate picture of risk, improve fraud and money laundering detection, and reduce the number of false positive transaction monitoring alerts.



# Nasdaq Verafin's Consortium Analytics Approach

## Profiling Within Our Consortium

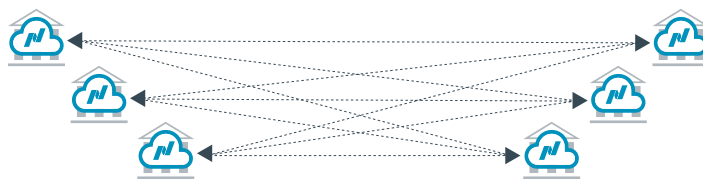
Nasdaq Verafin's consortium approach starts with Nasdaq Verafin ingesting rich demographic details and payment transactions from a financial institution. From these transactions we create account profiles, including statistical details for all payment channels for every account within our network of financial institution customers.



Nasdaq Verafin ingests rich data from a financial institution customer, collating details on payment behavior to assemble an account that is specific to each entity at the institution.

## Profiling Beyond Our Consortium

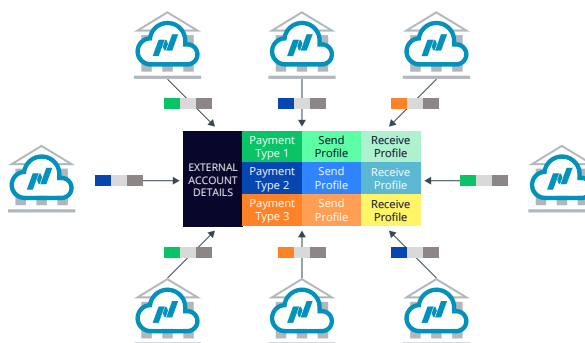
As institutions interact with accounts outside our consortium, Nasdaq Verafin uses the outgoing and incoming payments from our consortium institutions to profile these external accounts.



Nasdaq Verafin repeats this account profiling process across all 2500 financial institutions in the consortium, and for entities at institutions outside the consortium.

## Building External Account Profiles

Leveraging these interactions across all institutions in the consortium, Nasdaq Verafin builds external account profiles — giving our financial institution partners a more complete picture of risk across the entirety of a transaction.

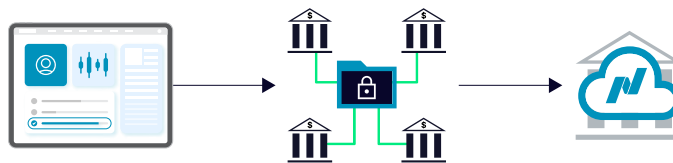


To assemble account profiles for entities outside the consortium, Nasdaq Verafin gleans and collates information from incoming transactions.

# Nasdaq Verafin's Consortium Analytics Approach

## Delivering Highly Accurate Results

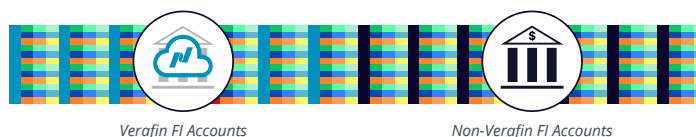
Providing evidence-based risk scores via web application and RESTful APIs allows Nasdaq Verafin to deliver the collective intelligence of the consortium directly to individual institutions without sharing the underlying information from financial institutions that helped produce the insight — this includes the protection of PII.



Consortium analytics examine these account profiles securely and discretely, delivering anonymized insights based on the collective intelligence of the consortium to Nasdaq Verafin's institution customers — without ever sharing PII.

## Confronting Financial Crime Challenges

Consortium data and analytics provide financial institutions with a powerful framework to address financial crime challenges — a framework that cannot be achieved by a single institution acting alone.



Using the collective insights from 650 million counterparty profiles, Nasdaq Verafin's consortium analytics provide financial institutions with a holistic understanding of risk across payments.

## Data Integration and Technology

For over twenty years, Nasdaq Verafin has developed deep domain expertise in fraud and money laundering typologies to detect and disrupt financial crime. With 2500 transaction monitoring customers in the Nasdaq Verafin Cloud, we have created a secure data lake of standardized, rich data representing more than \$9 trillion USD and 650 million counterparty profiles.

Nasdaq Verafin has successfully integrated with financial services data systems including core data, ancillary data, open-source data, third-party data, and consortium data, and standardized demographic and transactional information from hundreds of sources, thousands of times. Through our experience and expertise, Nasdaq Verafin has become an industry leader in data integration, transformation, and standardization, enabling us to develop and deliver highly effective solutions for fraud, money laundering, and compliance challenges faced by financial institutions.

2500  
transaction monitoring customers  
in the Nasdaq Verafin Cloud

with rich data  
representing more than  
\$9T USD

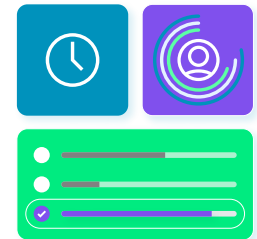
and  
650 Million  
counterparty profiles

Nasdaq Verafin leverages API integrations and batch files in various formats and frequencies, which includes customized data extracts as well as industry standard data formats such as Check21, NACHA, Fedwire, SWIFT, and ISO8583.

The result is a secure data lake with a defined data model for input from multiple institutions, where all relevant customer and transactional information is standardized, but linked to the original system of record for strong data lineage and validation. This rich data store is organized, scalable, and accessible for analysis — regardless of data source. Our unique consortium data set, with standardized and anonymized data from a wide range of institutions in the Nasdaq Verafin Cloud, enables the development of innovative consortium analytics — unachievable with the limitations of a single institution's data.

### Data and Counterparties

Advanced technology combined with our immense set of rich data provides Nasdaq Verafin with unprecedented analytical capability. Account, demographic and financial institution information is extracted from wire, ACH, instant payment and other rich transaction data in our cloud-based consortium data set in the Nasdaq Verafin Cloud. The strength of this standardized data enables Nasdaq Verafin to deliver comprehensive anti-financial crime consortium analytics and solutions delivering a more complete picture of customers' transactions, interactions, and relationships, including non-customer counterparties. Using information extracted from the rich data across the Cloud, Nasdaq Verafin resolves details about entities to form counterparty profiles, helping investigators expedite reviews with enhanced insights into customer and counterparty risk.



Expedite reviews with enhanced insights into customer and counterparty risk.

### Protecting Privacy with Nasdaq Verafin

Nasdaq Verafin's consortium analytics safeguard the privacy of all contributing financial institutions and their customers. When data is analyzed across our unique consortium network, PII is never shared with other institutions. Anonymized data is analyzed across the consortium, identifying patterns of suspicious activity, reducing false positive alerts, and increasing efficiency by reducing unnecessary reviews that slow down a transaction. Consortium-level insights are delivered back to all participating institutions through Nasdaq Verafin's Financial Crime Management platform in the form of account and counterparty risk scores.

Consortium data is critical in deploying innovative and collaborative approaches to identify patterns of criminal activity, evolving trends, and financial crime risks more effectively across institutions to ultimately disrupt crime. Insight into known, low-risk counterparty accounts across the consortium reduces false positive alerts, improves investigator efficiency, and reduces customer friction as payments to these counterparties can proceed in real-time. Financial institutions are alerted to higher-risk transactions that require enhanced due diligence and pose a greater risk to their institution and their customers, empowering investigators to focus on higher-risk activities that are more likely to be fraud.

## Proof of Concept: Consortium Analytics

In a recent wire fraud Proof of Concept with a top five U.S. bank, Nasdaq Verafin delivered a 25% false positive alert reduction and a 250% improvement in wire fraud detection by value with consortium analytics.

25%  
reduction



250%  
improvement



### Consortium Analytics Use Case: AML Investigations



*Assessing counterparty risk is a key piece of an AML investigation — the counterparty your customer interacts with can be the deciding factor between a low- and high-risk AML alert. Typical transaction monitoring often focuses on customer details and transactional activity, looking for patterns resembling criminal typologies, with counterparty risk assessment as an afterthought.*

Investigation teams spend time and resources researching and documenting counterparty risk, even when the counterparty has an established history of low-risk activity. Multiple investigators may spend time researching and investigating the same counterparty multiple times, wasting valuable time and resources within an institution. Counterparty research can account for up to 60% of investigation time during alert reviews – high volumes of alerts requiring counterparty research can overwhelm investigators and delay decision-making.

Leveraging consortium data, consortium analytics can effectively determine counterparty risk to create a profile of every entity that your customers bank or interact with. Over 2400 financial institutions populate Nasdaq Verafin's consortium data set – our consortium analytics automatically determine the risk associated with entities, counterparties, and transactional relationships. By incorporating these insights, consortium analytics provide investigators with unique insights into counterparty risk so investigators can prioritize their investigative efforts to focus their time on high-risk counterparties and reduce the amount of time spent investigating low-risk counterparties.

## Consortium Analytics Use Case: Money Mules



*Nasdaq Verafin's consortium approach provides valuable insight by profiling both the payment originator and the beneficiary. We extract information from thousands of financial institutions to profile hundreds of millions of counterparties with rich demographic and transactional data. Consortium analytics are deployed to analyze the anonymized data across our consortium network to identify patterns of suspicious activity and assess risk across accounts, counterparties, and transactions.*

With over 575 million counterparties profiled across our consortium network, Nasdaq Verafin identifies potential money mule accounts to alert institutions to risk. As payments are identified as known or suspected fraud, these potential money mule accounts are flagged for future risk to protect all financial institutions in the consortium. Similarly, receivers with a history of legitimate activity are identified as lower risk, making it easier for the institution to allow payments to these accounts to proceed.

As part of the Nasdaq Verafin consortium, a single institution is alerted when a payment should be interdicted or elevated for enhanced due diligence, and false positives can easily be explained away. The institution gains all the benefits of collaboration by deploying Nasdaq Verafin's consortium analytics, without directly collaborating themselves.

## Consortium Analytics Use Case: Combating Payments Fraud



*Payments fraud is a major concern in the financial industry. With customers expecting fast, frictionless transactions and the increasing presence of real-time, instant payment options, financial institutions have a narrow window of opportunity to detect and interdict suspicious transactions. Fraudsters are also targeting vulnerable populations, such as seniors, and using lucrative authorized push payment scams to manipulate customers into initiating fraud themselves, rendering most password and token controls ineffective. Meanwhile, siloed approaches to prevention have contributed to overwhelming false positive alerts at many financial institutions — further hampering anti-financial crime efforts.*

Using insights from over 650 million counterparty profiles, Nasdaq Verafin's consortium analytics consider the complete picture of risk across the entirety of a transaction. Payments involving known accounts with a history of legitimate activity across the consortium are analyzed as lower risk, while payments involving unrecognized accounts are analyzed as higher risk — representing potential mules or other accounts opened to facilitate fraud. This allows financial institutions to consider the risk of the accounts on both sides of a payment to improve fraud detection and reduce false positives, customer friction, and operational costs.

### Leading the Change

Consortium analytics offers a holistic solution for both fraud and AML investigations. Verafin's unique consortium data set and innovative consortium analytics empower financial institutions with a secure collaborative framework to fight financial crime.

As criminals continue to seek new technologies and tactics to target financial institutions and customers across the globe, it is critical that institutions work together to disrupt both lone bad actors and criminal organizations. Financial institutions need to adopt this unified consortium approach to work together to detect and successfully disrupt financial crime.



Nasdaq Verafin provides cloud-based Financial Crime Management Technology solutions for Fraud Detection, AML/CFT Compliance, High-Risk Customer Management, Sanctions Screening and Management, and Information Sharing. More than 2,500 financial institutions globally, representing more than \$9T in collective assets, use Nasdaq Verafin to prevent fraud and strengthen AML/CFT efforts. Leveraging our unique consortium data approach in targeted analytics with artificial intelligence and machine learning, Nasdaq Verafin significantly reduces false positive alerts and delivers context-rich insights to fight financial crime more efficiently and effectively.

**To learn how Nasdaq Verafin can help your institution fight fraud and money laundering visit [www.verafin.com](https://www.verafin.com) or call 1-877-368-9986.**

© 2025 Nasdaq, Inc. All rights reserved.

Nasdaq, the Nasdaq logo, and Verafin are registered and unregistered trademarks, or service marks, of Nasdaq, Inc. or its subsidiaries in the U.S. and other countries.

