VERAFIN
A STEP AHEAD

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 check, 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[1] while crimes against consumers increases.[2] Criminals, unconstrained by privacy rules, government regulations, technology, and geographic boundaries have unlimited access to dark web technology, to buy and sell personal identifiable information (PII) and share information. 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

Financial institutions are spending more every year on anti-money laundering and fraud detection. In 2020, global banks were hit with $10.4 billion in fines for money-laundering violations, an increase of more than 80% from 2019,[3] and the cost of compliance and risk mitigation over the last eight years has increased by over 60 percent for retail and corporate banks.[4]

Meanwhile payments fraud loss continues to impact both financial institutions and customers alike. Authorized Push Payment (APP) fraud has quickly become a preferred method of attack across the globe,[5] 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.

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 The Economist, The War Against Money-Laundering is Being Lost, 2021, https://www.economist.com/finance-and-economics/2021/04/12/the-war-against-money-laundering-is-being-lost

4 Deloitte, Regulatory productivity: Is there an answer to the rising cost of compliance?, 2023, https://www2.deloitte.com/us/en/pages/regulatory/articles/cost-of-compliance-regulatory-productivity.html

5 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 July 2023, the U.K. Payment Systems Regulator (PSR) announced new requirements for banks to ensure that APP fraud victims are reimbursed; however, a subsequent U.K. Supreme Court ruling stated that banks cannot be held responsible for fraudulent transactions when a customer authorized the payment from their account.[6]

In the United States, citizens are victimized in record numbers — the FTC reports consumers lost nearly $9 billion in scams in 2022, a 30% increase from 2021.[7] Verafin's Q2 2023, Quarterly Cloud Insights: Wire Fraud Benchmarking report[8] shows attempted wire fraud for both persons under 55 and the elderly increased by occurrences and value from Q4 2021 to Q4 2022. The mean and median value of attempted wire fraud against individuals increased, with the median rising from $9.9K to $12K, and the mean saw a significant increase during this timeframe from $26.5K to $31.6K.

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.,[9] 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 is 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.

6 Bloomberg, UK Banks Not Liable for Fraud If Clients Authorized Payment, https://www.bloomberg.com/news/articles/2023-07-12/uk-banks-not-liable-for-frauds-if-customers-authorized-payments?leadSource=uverify%20wall, 2023

7 Federal Trade Commission, New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

8 Verafin, Quarterly Cloud Insights Q2 2023 Wire Fraud Benchmarking Report, 2023, https://verafin.com/resource/quarterly-cloud-insights-q2-2023-report/

9 United States Senate, Letter the Consumer Financial Protection Bureau, 2022, 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 both sides of a transaction, the originator and the beneficiary, 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.

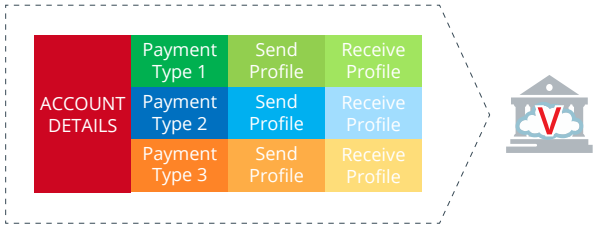
Consortium analytics provide a unique and essential contribution to managing and preventing financial crime. When criminals collaborate, sharing malicious practices and evading detection, consortium analytics and counterparty analysis offer financial institutions an approach to benefit from collective 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.

Verafin's Consortium Analytics Approach

Profiling *Within* Our Consortium

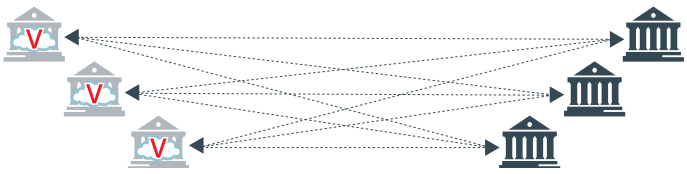
Verafin's consortium approach starts with a single Verafin financial institution sending rich demographic and payment transactions. From these transactions we create account profiles, including statistical details for all payment channels for every account within our network of financial institution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



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

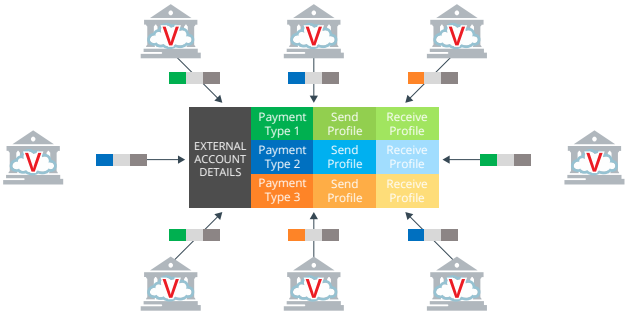
As institutions interact with accounts outside our consortium, Verafin uses the outgoing and incoming payments from our consortium institutions to profile these external accounts.



Verafin repeats this account profiling process across all 2400 financial institutions in the consortium, and for entities at institutions outside the consortium.

Building External Account Profiles

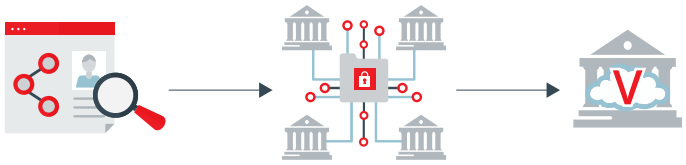
Leveraging these interactions across all institutions in the consortium, Verafin builds external account profiles — giving our financial institution partners a more complete picture of risk across the entirety of a transaction.



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

Delivering Highly Accurate Results

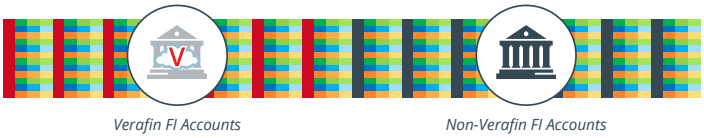
Providing evidence-based risk scores via web application and RESTful APIs allows Verafin to deliver the collective intelligence of the consortium directly to individual institutions without sharing the underlying information from financial institutions that helped produce the insight — this includes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



Consortium analytics examine these account profiles securely and discretely, delivering anonymized insights to Verafin's financial institution customers that are based on the collective intelligence of the consortium 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 575 million counterparty profiles, Verafin's consortium analytics provide financial institutions with a holistic understanding of risk across payments.

Data Integration and Technology

For over twenty years Verafin has developed deep domain expertise in fraud and money laundering typologies to detect and disrupt financial crime. With 2400 transaction monitoring customers in the Verafin Cloud, we have created a secure data lake of standardized, rich data representing more than $4.5 trillion USD and 575 million counterparty profiles.

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, 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.

2400
transaction monitoring customers *in the Verafin Cloud with* ***rich data representing*** *more than*
$4.5T USD
and
575 Million
counterparty profiles.

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 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 Verafin with unprecedented analytical capability. Account, demographic and financial institution information is extracted from wire, ACH, check and other rich transaction data in our cloud-based consortium data set in the Verafin Cloud. The strength of this standardized data enables 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, 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 Verafin

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 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.

Consortium Analytics Use Case: Check Fraud

Effectively responding to fraudulent checks, including stolen and altered check fraud scams, requires collaboration between financial institutions on both the depository and in-clearing sides of a transaction.

Consortium analytics identifies stolen check fraud collaboratively, without sharing PII between institutions. By leveraging fraud alerts on the deposit side of the transaction, to uncover the risk related to the deposit account, Verafin's Deposit Fraud analytic alerts investigators that a check deposited at Bank A is potentially fraudulent and a hold is placed.

When the check arrives at Bank B, Verafin's Check Fraud Consortium Analytics references our unique consortium data set to link the deposit fraud to the in-clearing check fraud, triggering an alert. A notification is sent to the in-clearing financial institution, Bank A, that a check drawn on one of its accounts is likely fraudulent, allowing investigators to verify the check authenticity, resulting in minimal loss.

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 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

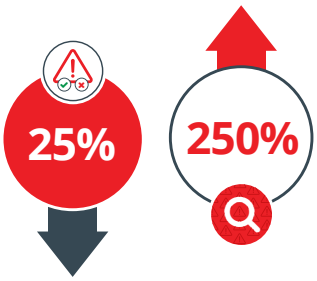
Verafin's consortium approach provides valuable insight by profiling both the payment originator and the beneficiary. We extract information from thousands of financial institutions to profile hundreds of millions of counterparties with rich demographic and transactional data. Consortium analytics are 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, 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 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 Verafin's consortium analytics, without directly collaborating themselves.

Proof of Concept: Consortium Analytics

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



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 575 million counterparty profiles, 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 collaborate and work together to detect and successfully disrupt financial crime.

About Verafin

Verafin, a Nasdaq company, offers enterprise Financial Crime Management solutions, providing a cloud-based, secure software platform for Fraud Detection and Management, AML/CFT Compliance and Management, High-Risk Customer Management, Sanctions Screening and Management, and Information Sharing. More than 3800 financial institutions use Verafin to effectively fight financial crime and comply with AML/CFT regulations. Leveraging our unique consortium approach, Verafin significantly reduces false positive alerts, delivers context-rich insights, and uncovers more financial crime. Verafin is proud to have industry endorsements in 48 U.S. states. To learn how Verafin can help your institution fight fraud, money laundering, and predicate crimes such as human trafficking and Business Email Compromise.

Learn more

For more information on this topic, or how Verafin can help your institution stay a step ahead of financial crime, call 866.781.8433.

To access Verafin's archive of webinars, white papers, success stories and other materials focusing on AML/CFT compliance and fraud detection topics relevant to financial institutions across the country, check out our online Resource Center at **www.verafin.com**.

VERAFIN
A STEP AHEAD