KROTON Platform Compliance Report – CIRO Rules Alignment

This report cross-reference KROTON software modules and **Investment Dealer and Partially Consolidated Rules (IDPC)** document of the Canadian Investment Regulatory Organization (CIRO) rulebook effective January 1, 2023, which applies to any company regulated as a CIRO Dealer Member. Key compliance areas from this rulebook – *Know Your Client (KYC) & suitability*, *sanctions and blacklist screening*, *trade surveillance* (e.g. spoofing, layering, wash trading, insider trading), and *audit trail, recordkeeping & supervision* – are analyzed below. The report also describes how the **KROTON compliance platform** supports the regulated companies in meeting these specific requirements.

Summary Table of CIRO Requirements and KROTON Compliance Solutions

Compliance Area	Relevant Rules	KROTON Modules	How Each Module Addresses the Rules
Know-Your-Client (KYC) & Suitability	• 3202 *Know-Your-Client* • 3402 Retail Suitability	KYC Miner	Captures full client identity & risk data, assigns dynamic risk scores, and integrates KYC, sanctions, and trading alerts so suitability reviews always reflect the latest client profile.
Sanctions & Blacklist Screening	• 3926(2)(iii) AML Obligation • 3202(1)(i) Reputation Inquiry • 3205 (No shell banks)	Sanctions Miner, RUMI Adverse-Media	Daily list synchronization plus algorithmic matching (Sanctions Miner) and real-time adverse-media sweeps (RUMI) surface true risk signals while cutting false positives—keeping firms onside with OSFI, UN, OFAC and PCMLTFA duties.
Trade Surveillance (Spoofing, Layering, Insider Trading, etc.)	• 3945 Retail Trade Supervision • 3950 Institutional Supervision	Scenario Manager	Custom rule sets in Scenario Manager flag manipulative patterns (spoofing/layering, wash trades, front-running, insider-trade indicators). All alerts flow into Case Manager for investigation, dual-level approval, and evidencing of daily/monthly reviews.
Record-Keeping, Audit Trail & Supervision	• 3801 / 3803 Record-Keeping • 3925 Supervision • 3927(2) Evidence of Reviews • 3955(3) Audit-Trail (OEO)	Scenario Manager, Built-in Audit Logs	Every alert, review, note and approval is time-stamped, immutable and retained ≥ 7 years. Supervisory logs and reports provide regulators with a complete audit trail on demand.

Know Your Client (KYC) and Suitability Compliance

CIRO KYC Requirements: The CIRO rules require performing diligent **Know Your Client (KYC)** procedures for every account. **Rule 3202** *"Know-Your-Client"* mandates that the firm **identify each client** and verify key personal details, making inquiries into the client's reputation if there is any cause for concern. The firm must determine if the client is a reporting insider and must collect enough information on the client's personal and financial circumstances, investment objectives, risk tolerance, and time horizon to meet its suitability obligations. In practice, this means the regulated company must have a complete client profile on file – including identity verification, employment and financial information, investment knowledge, risk profile, etc. – and keep this information **current**. **Rule 3202** also requires a new account application for each client and prompt confirmation of the collected information's accuracy by the client.

CIRO Suitability Requirements: Beyond gathering KYC data, CIRO rules obligate the companies to **use that data to ensure suitability** of investments. **Rule Group 3400** (Suitability Determination) and its subsections specify that **before any trade, recommendation, or discretionary decision**, the dealer must determine on a reasonable basis that the action is *suitable for the client* and **puts the client's interest first**. For retail clients, **Rule 3402** lays out that suitability must be assessed in light of the client's KYC profile (as collected under **Rule 3202**) and the characteristics of the investment product. Factors such as the concentration of the investment in the client's portfolio, liquidity, and the costs and benefits of the transaction must be considered, as well as a reasonable range of alternative actions available. In essence, the company must **match clients to appropriate investments**: no trade should be made unless it is appropriate for the client's financial situation and objectives, and any advice given must prioritize the client's best interest. CIRO also requires that certain triggering events (like significant changes in the client's circumstances or portfolio) prompt a fresh suitability review of the account.

KROTON Platform – KYC Data Management: The **KROTON compliance platform** greatly enhances your company's ability to meet KYC obligations. Using the **KYC Miner** tool, the company can digitally capture and monitor all essential client information in one place. KROTON's KYC Miner is designed for *"flexible and precise customer risk evaluation,"* allowing the firm to implement **customizable risk scoring** models based on a wide range of client parameters. This means that one can assign each client a risk profile (low, medium, high risk, etc.) by inputting factors like income, net worth, investment experience, and even behavioral indicators. The platform supports **dynamic risk re-evaluation** – as client information changes or as time passes, **KROTON automatically triggers re-assessments** of the client's risk score and KYC details on a schedule or when certain events occur. This helps the company remain compliant with the requirement to *remain informed* of clients' current circumstances.

Moreover, KROTON provides **KYC 360° Dashboards** which give compliance officers and advisors a holistic view of each customer's risk and compliance status. These dashboards present *"integrated views of Customer Due Diligence (CDD), Sanctions Screening, and Transaction Monitoring"* in one interface. In practice, when a representative pulls up a client's profile in KROTON, they can see not only the basic KYC data but also whether that client has any sanctions or politically exposed person flags, and any

alerts from transaction monitoring. This comprehensive risk profile aligns with CIRO's expectations that firms know all essential facts about their clients. The dashboard also offers **detailed investigative tools** – for example, staff can drill down into *historical details and risk trends* for an individual client over time. This makes it easier to spot if a client's situation has changed (e.g., a shift in trading patterns or new risk factors), ensuring that the system can update the KYC information and reassess suitability promptly.

KROTON Platform – Suitability Controls: With robust KYC data in place, KROTON aids in **ensuring suitability** of trades. The platform can be configured with rules and AI models that compare any proposed investment or order against the client's profile. For instance, if an advisor attempts to place a trade that would overly concentrate a client's portfolio in a single high-risk security, KROTON can flag this as *potentially unsuitable*. By leveraging the client's risk score and investment objectives (stored via KYC Miner), the system can generate alerts for off-profile transactions – such as a trade that exceeds the client's risk tolerance or an aggressive option trade in a conservative account. KROTON's **scenario management** module also integrates KYC risk levels into its monitoring algorithms. That means clients with higher risk scores might trigger stricter scrutiny on trades, aligning with a risk-based approach.

Additionally, KROTON helps evidence compliance with suitability obligations. Every time an account's suitability is reviewed (whether due to a material change or a periodic review), the platform can log the review action. Supervisors can use the system to document that they have approved a new account or a product recommendation for a client after verifying it meets CIRO's criteria. This creates a record (with timestamps and reviewer names) that the company can show to regulators to demonstrate it is following **Rule Group 3400.** In short, **KROTON operationalizes KYC and suitability** – it ensures the company collects all necessary client info, keeps it updated, calculates client risk profiles, and uses those profiles to automatically check the appropriateness of investments, thereby embedding CIRO's KYC and suitability requirements into daily practice.

Sanctions and Blacklist Screening Compliance

CIRO Requirements (Sanctions & AML): Although the CIRO rulebook focuses on investment dealer rules, it explicitly requires firms to adhere to all anti-money laundering (AML) and anti-terrorist financing laws. CIRO **Rule 3926(2)** mandates that Dealer Members' supervision policies *"specifically address the obligations to… (iii) comply with all anti-money laundering and terrorist financing requirements under applicable laws."*. In the Canadian context, this means one must follow the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and related regulations, which include obligations to perform sanctions screening and prevent dealings with sanctioned individuals or entities. Separately, as part of KYC due diligence, **Rule 3202(1)(i)** implies that if there is any reason to doubt a client's integrity or if a client is from a high-risk jurisdiction, the firm should make *"reasonable inquiries as to the reputation of the client."* In practice, such inquiries include checking whether the client appears on any **sanctions lists (e.g. UN, OSFI, or other global lists)** or is known to be associated with criminal or terrorist activities. CIRO's rules also forbid opening accounts for **anonymous or untraceable entities** – for example, **Rule 3205** prohibits dealing with "shell banks" (banks with no physical presence), a measure directly aimed at preventing terrorist financing. Thus, one must have robust controls to screen new and existing clients against applicable sanctions, terrorist lists, and other blacklists (like those for fraud or organized crime), and to monitor transactions for any hits, and continuously monitor adverse media for existing clients.

KROTON Platform – Sanctions Screening: The **KROTON platform's sanctions screening capabilities** ensure that the companies under CIRO regulation stay fully compliant with these obligations. KROTON includes a dedicated **Sanctions Miner** module which provides *"rigorous compliance with global standards."* This tool **monitors and screens client data against all major international and domestic sanctions lists**, which are updated on a daily basis. In practice, the system will automatically cross-check names of new clients, as well as counterparties in transactions, against lists such as the Canadian OSFI Consolidated Sanctions List, US OFAC lists, United Nations sanctions, EU/UK sanctions, and other relevant databases. The comprehensive list coverage means the users can be confident it isn't missing a lesser-known local list or a sector-specific blacklist – KROTON handles updates to all these sources and keeps the database current without manual intervention.

KROTON's sanctions screening is highly automated and intelligent. The platform boasts *"automated integration"* with sanctions list providers (for example, it can plug into Refinitiv World-Check or Dow Jones Watchlists) to fetch updates and perform checks seamlessly. This integration allows real-time or batch screening in the background – for instance, if a new name is added to a sanctions list overnight, KROTON will flag any matching client by the next morning, if not immediately. The system supports **multiple screening modes** (full database scans, daily incremental/delta scans, on-demand checks for individual names, and real-time API calls). This flexibility enables the compliance team to schedule regular sweeps of the entire client base and also to trigger instant checks when needed (for example, if a prospective client walks in, their name can be screened instantly before account opening). Since the global and national lists are updated on a daily basis, it is imperative to do these checks on a daily basis.

A critical challenge in sanctions compliance is handling false positives – common names or partial matches can generate "hits" that aren't true matches to sanctioned parties. KROTON addresses this with advanced matching technologies to improve accuracy. By doing so, KROTON reduces the noise, allowing the compliance officers to focus on genuine threats. The platform employs **natural language processing (NLP) for risk scoring** of name matches. This means when a potential name match is found, KROTON can assign a similarity/confidence score (taking into account variations, spelling differences, etc.) to help analysts decide if it's a true match. It can even incorporate secondary information – for example, if the location or birthdate of the client differs from the sanctioned individual's data, the system can flag it as low probability, whereas if several data points align, it flags high risk.

KROTON Platform – Case Handling for Sanctions: When a sanctions or blacklist alert does occur, KROTON's **Case Manager** ensures it is handled in compliance with regulations. The alert is logged as a case with all the scores and match details so that an informed decision can be made.

Adverse-Media Intelligence Layer: To give sanctions screening fuller context and capture broader reputational risk, KROTON can bolt on its **RUMI Adverse-Media module** to all sanctions hit. When a potential match is flagged, RUMI automatically queries thousands of curated sources—regulatory-enforcement sites, investigative journalism, **mining related news**, NGO blacklists, ESG-watch portals, and multilingual news feeds—for any negative coverage tied to the name, its close associates, or related entities. Results (articles, leaked-data mentions, enforcement actions) are scored by NLP for relevance and severity, then surfaced inside the same results view, enabling analysts to see—at a glance—whether the individual or company is connected to corruption probes,

environmental violations, terrorist financing networks, or other red-flag behaviour. Because RUMI's index refreshes several times daily, compliance staff receive near-real-time alerts when fresh adverse media appears—helping them validate true sanctions matches faster, enrich SAR narratives, and uncover high-risk but not-yet-listed actors that could endanger any CIRO dealer's reputation.

In summary, **KROTON fortifies sanctions screening program** by providing up-to-date list coverage, smart matching algorithms to minimize false positives, and integrated workflows for resolving alerts. These capabilities align directly with CIRO's mandate that dealers comply with AML/CTF laws. The users can thus confidently prevent opening accounts for or doing business with any person or entity on sanctions/terrorist lists, and it can rapidly respond to any sanctions-related risks that arise, in full accordance with regulatory expectations.

Trade Surveillance (Spoofing, Layering, Wash Trading, Insider Trading)

CIRO Requirements (Trade Supervision): CIRO rules impose a comprehensive duty on dealer members to supervise trading and detect **market abuses**. **Rule 3945(2)** lists specific forms of improper trading that the company's policies and procedures must be capable of **detecting**, including: *"unsuitable trading, undue concentration, excessive trading, trading in restricted securities, conflicts of interest between staff and client trading, unauthorized trading indicators, inappropriate or high-risk strategies, deterioration of account holdings, improper crosses, employee trading abuses, front-running, [and] manipulative and deceptive activities"* as well as **insider trading**. Notably, *"manipulative and deceptive activities"* encompass schemes like **spoofing** (placing fake orders to manipulate prices), **layering** (placing and cancelling orders to trick the market), **wash trading** (buying and selling the same asset to create false volume), and other forms of market manipulation. Insider trading – trading on material non-public information – is explicitly identified as a prohibited activity that must be surveilled. For institutional accounts, **Rule 3950** imposes a similar requirement: the firm's supervisory procedures must *"specifically address detecting improper or suspicious account activity including: (i) manipulative and deceptive activities, … (iv) front running, … and (vii) exceeding position limits,"* among others. In essence, CIRO expects the company to have **active trade surveillance systems** and processes to **monitor all client trading and employee trading**, and to flag any patterns suggestive of market manipulation, insider dealing, or other improper practices.

To comply, the company must perform **daily** and **monthly reviews** of trading activity (per **Rule 3945(1)**) and investigate any red flags. The firm should have automated alerts or reports for things like a sudden spike in trading activity, accounts trading the same stock in coordination (possible collusion or wash trades), orders that are entered and cancelled at high frequency (possible spoofing), or accounts trading ahead of client orders or news (front-running or insider trading). CIRO rules also demand that evidence of these supervisory reviews be maintained. The breadth of items in the rules shows that the regulator expects a dealer to catch even subtle forms of abuse.

KROTON provides a **Scenario Manager** (custom flexible rule-based monitoring) and a **Case Manager** (alert handling and documentation) to meet all trade surveillance requirements. In this framework, scenario rules define suspicious-trade patterns and Case Manager drives investigation workflows and record-keeping. Together they let the compliance team perform daily and monthly trade reviews (per CIRO's **Rule 3945**) and detect manipulative or insider trading with no additional "black box" modules. Scenario Manager rules can be configured to flag *spoofing/layering* (non-bona-

fide order patterns) and *insider trading* signals, and Case Manager ensures every alert is investigated, approved, and documented.

Scenario Manager (Rule-Based Monitoring)

- **Custom Scenarios:** Define precise trading scenarios by instrument, account, trader, order type, time, etc. Scenario rules are fully configurable and can incorporate business logic (e.g. account risk level or client type). KROTON supports *scheduled scenario runs* – for example, rules can run automatically each trading day after market close or on a set monthly schedule. This ensures continuous compliance without manual intervention (meeting CIRO's expectation that daily reviews catch **Rule 3945** issues).
- **Spoofing/Layering Detection:** Build rules to detect rapid patterns of non-bona-fide orders and cancellations – the classic spoofing/layering scheme. CIRO/IIROC explicitly classifies spoofing and layering as manipulative trades, so Scenario Manager can target them by flagging when a trader places large orders they quickly cancel (especially one-sided orders followed by opposite-side trades). Such scenarios might look for short time intervals between order placement and cancelation on one side of the book, or patterns of laddered orders at multiple price levels (layering).
- **Insider Trading Signals:** Include rules that monitor for insider-type activity. For example, scenario logic can cross-reference trades with lists of insiders, or watch for employee and associated accounts buying/selling around announcements. Trade surveillance's goal is explicitly to detect "insider trading" and other misconduct. By configuring scenarios on personal or proprietary accounts (e.g. employees, control persons), Scenario Manager can flag unusual P&L or trading just before news events. Any alert can then be examined as a potential insider trading case.
- **CIRO Daily/Monthly Reviews:** Scenario Manager can automate the required CIRO first-tier reviews. For daily supervision, a scenario can be set to run "one business day after" each trading day, checking the prior day's retail trades for the specific issues listed in **Rule 3945**. For example, rules can look for large price moves, wash trades, or high-commission accounts in the past day. Monthly scenarios can select accounts by risk criteria (CIRO suggests reviewing clients with high commissions or large cash flows) and flag any unusual activity. In this way the company can satisfy CIRO's requirement to review all accounts with significant trading each month. All scenarios – daily or monthly – are built in Scenario Manager's rule engine, giving supervisors full control over thresholds and conditions.
- **Automated Alerts:** When a scenario condition is met, Scenario Manager automatically generates an alert. This aligns with CIRO guidance that firms may rely on automated alerts for manipulative trading. Each alert is tagged with the triggering rule and all relevant trade details. This enables immediate filtering of issues worth investigating (e.g. confirmed spoofing signals or odd insider trades) and avoids time-consuming manual data sifting. Automated alerting means no suspicious pattern is missed and every matched scenario is escalated to Case Manager.

Case Manager (Investigation & Documentation)

- **Case Creation & Workflow:** All alerts from Scenario Manager flow into KROTON's Case Manager. The system *automatically creates cases* for each alert, organizing them into a unified

dashboard. Compliance staff then follow defined workflows to investigate each case. KROTON supports robust approval processes (e.g. two-level supervisory sign-off) on every case, ensuring nothing is closed without proper review. This automated case orchestration means the company can prove an audit trail of reviews in line with CIRO's expectations.

- **Investigation Tools:** Within each case, investigators have full visibility into the related trades and accounts. They can drill down into detailed trade lists, order histories, customer profiles, and any linked parties. Case Manager allows attaching notes, documents, or screenshots directly to the case. For example, if a spoofing alert is raised, the investigator can attach order books, client communications, or market data to explain the finding. All relevant evidence stays connected to the case, making the root cause clear.
- **Documentation & Audit Trail:** Every action on a case is logged. Case Manager records who reviewed or dismissed an alert, what notes were added, and what the outcome was. Investigators can mark cases as "false positive" or "escalated to regulator", and the system retains that disposition. This complete audit trail means the company has documented proof of its compliance efforts – for example, showing that **Rule 3945** alerts were reviewed within one day and monthly account checks were done within **21 days**. In a CIRO examination, supervisors can easily generate reports from Case Manager to demonstrate that every scenario-generated alert was addressed in accordance with policies.
- **Regulatory Compliance:** Case Manager also supports CIRO reporting needs. It can generate summary reports or logs of all cases closed in a period, showing that the daily/ monthly supervision was performed. Because KROTON Case Manager stores all case materials and approvals, the company can compile evidence (screenshots, approvals, investigator notes) needed for audits of trading supervision. In short, Scenario Manager catches potential issues via rule logic, and Case Manager drives them to resolution with full documentation.

Overall, KROTON's Scenario Manager and Case Manager together give the companies a complete compliance solution. Scenario Manager's configurable rules ensure that **spoofing, layering, insider trading, wash trades, and other manipulative patterns** are automatically detected. Case Manager then ensures each alert is properly investigated, approved, and recorded. This dual-module setup fully satisfies CIRO trade surveillance requirements (including Rule 3945 daily/monthly reviews) using only these two KROTON components.

Audit Trail, Recordkeeping, and Supervision Obligations

CIRO Requirements (Records & Supervision): CIRO's rules emphasize that maintaining proper records and a strong supervisory system is a core responsibility of a dealer member. Rule 3801 states that *"maintaining complete and accurate records is a fundamental responsibility"* and that such records **"provide an audit trail"** supporting the firm's supervision of its business. In other words, every aspect of the compliance and operations should be documented such that regulators can later reconstruct what happened. CIRO specifies a **minimum 7-year retention period** for all required records (trade blotters, statements, forms, supervision logs, etc.), unless laws demand longer. This includes records of KYC information, transaction records, and evidence of compliance reviews.

On the **supervision** side, **Rule 3925** requires the companies to *"effectively supervise account activity"* and take reasonable steps to ensure compliance with all regulatory requirements. The firm must designate qualified Supervisors for this task and have clear procedures for how supervision is carried out. Crucially, CIRO expects that **supervisory reviews are documented**. Rule **3927(2)** obliges firms to

"record and keep evidence of completed supervisory reviews, including details of inquiries about issues and their resolution," for the same retention period as other records (7 years). Additionally, in the context of order-execution-only accounts, CIRO **Rule 3955(3)** explicitly requires maintaining *"an audit trail of all supervisory reviews"* performed – underscoring that every review, whether automated or manual, should leave a trace that can be audited. Combined, these rules mean the company must have robust systems to **track compliance actions**: from the moment an account is opened, through each trade review, to any investigations or filings, there should be a reliable log.

Another aspect is **escalation and approval**. CIRO rules (e.g., **Rule 3947**) demand new registered representatives be subject to heightened supervision, and that new accounts are approved by a Supervisor on a timely basis. Supervisors also must approve any discretionary accounts and certain high-risk activities. All these supervisory decisions and approvals need to be recorded. Essentially, if an auditor asks "how do we know this trade was reviewed by compliance?" or "where is the sign-off for this new account?", the company should be able to produce records to answer that.

KROTON Platform – Audit Trails and Recordkeeping: The KROTON platform is designed with compliance recordkeeping in mind, ensuring that **every action is logged** and stored for future reference. In KROTON's **Case Manager and workflow system**, whenever a compliance officer reviews an alert or case, the system automatically captures who did it, when, and what the outcome was. For example, if Suspect Miner flags a suspicious trade and a compliance analyst investigates and concludes it's a false alarm, that conclusion (with the analyst's notes) is saved in the case file with a timestamp. These digital records constitute the **audit trail** that CIRO demands. They show that the compliance team is actively supervising and addressing issues. KROTON retains these logs in a durable form (database records, downloadable reports) that can be accessed even years later, satisfying the 7-year record retention requirement. In fact, the system's architecture ensures data backups and secure storage so that historical compliance data is not lost or tampered with.

One of KROTON's features is the **Dual-Level Approval Process** in case workflow, which directly supports good supervision practices. As noted in the platform documentation, KROTON *"implements a robust two-level approval system within the workflow, ensuring thorough review and oversight of all cases."*. In practical terms, this means certain sensitive compliance decisions (for instance, deciding to close an alert about a potentially serious issue, or filing an official report) must be approved by at least two people – typically the front-line compliance analyst and a senior compliance manager. The platform will not mark the case as resolved until the second approver signs off. This built-in control enforces the idea of **supervisory oversight** and prevents single-point failure (i.e., an analyst inadvertently ignoring a real problem). It also produces a clear record: both approvers' names and the time of approval are recorded in the case log. The company can thus demonstrate to regulators that a supervisor indeed reviewed and approved each resolution, which aligns perfectly with CIRO's expectations for supervision and escalation.

Comprehensive Case Documentation: KROTON's Case Manager encourages comprehensive documentation of each alert or investigation, which is critical for recordkeeping. The interface allows users to **attach documents, add notes, and link relevant transactions or customer information** to the case. For example, if investigating a potential insider trading incident, a compliance officer might upload research reports or email transcripts as evidence. All these attachments remain with the case record. The platform bulletins highlight *"Documentation and Tracking"* as a core feature, noting that it

maintains a comprehensive history for each case that can be accessed with ease. This means years later, if CIRO or another auditor asks about a specific alert from, say, 2024, the company can pull up that case in

Retention and Access: KROTON's data retention settings can be configured to align with the 7-year rule (or longer, if needed). By default, nothing is deleted from the compliance database unless deliberately purged by policy, so the company can keep an indefinite archive. And because KROTON is a digital system, retrieving records is far easier than digging through paper archives. A supervisor can search the system for all cases related to a particular client or a particular type of alert and get the history instantly. This capability is invaluable when responding to audits or regulatory inquiries. It allows the company to quickly demonstrate compliance by producing evidence of reviews and decisions.

In essence, **KROTON creates a living audit trail** of the compliance program. From KYC information gathering to trade surveillance alerts and their resolution, every step is captured. CIRO **Rule 3804** requires that records be kept to *"demonstrate the Dealer Member's compliance with… requirements"*, and KROTON ensures the compliance team can do exactly that. The platform's logs will show that the company conducted supervisory reviews as required (who looked at what, and when), that any issues were escalated appropriately (with management approvals documented), and that the firm can account for its actions over time. This level of recordkeeping and supervision significantly lowers the risk of compliance failures and provides confidence during regulatory examinations. Executive teams and supervisors can also use KROTON's reporting dashboards to oversee the overall compliance program, identifying trends (e.g., repeated issues with a particular registered representative or branch) and taking proactive action – fulfilling the CIRO requirement for effective supervision.

Conclusion: By aligning the KROTON platform's capabilities with the CIRO rulebook requirements, compliance teams can confidently ensure it meets all its compliance obligations. The KROTON platform, with its comprehensive suite of compliance tools, is well-suited to automate and reinforce adherence to these rules. Through proper use of KROTON's KYC Miner, Sanctions Miner, Scenario Manager, Adverse Media Search, and case management features, trading companies can maintain a strong compliance system that not only satisfies CIRO's current rules but is adaptable to future regulatory changes – all while keeping thorough records and audit trails of its efforts as evidence of compliance.