

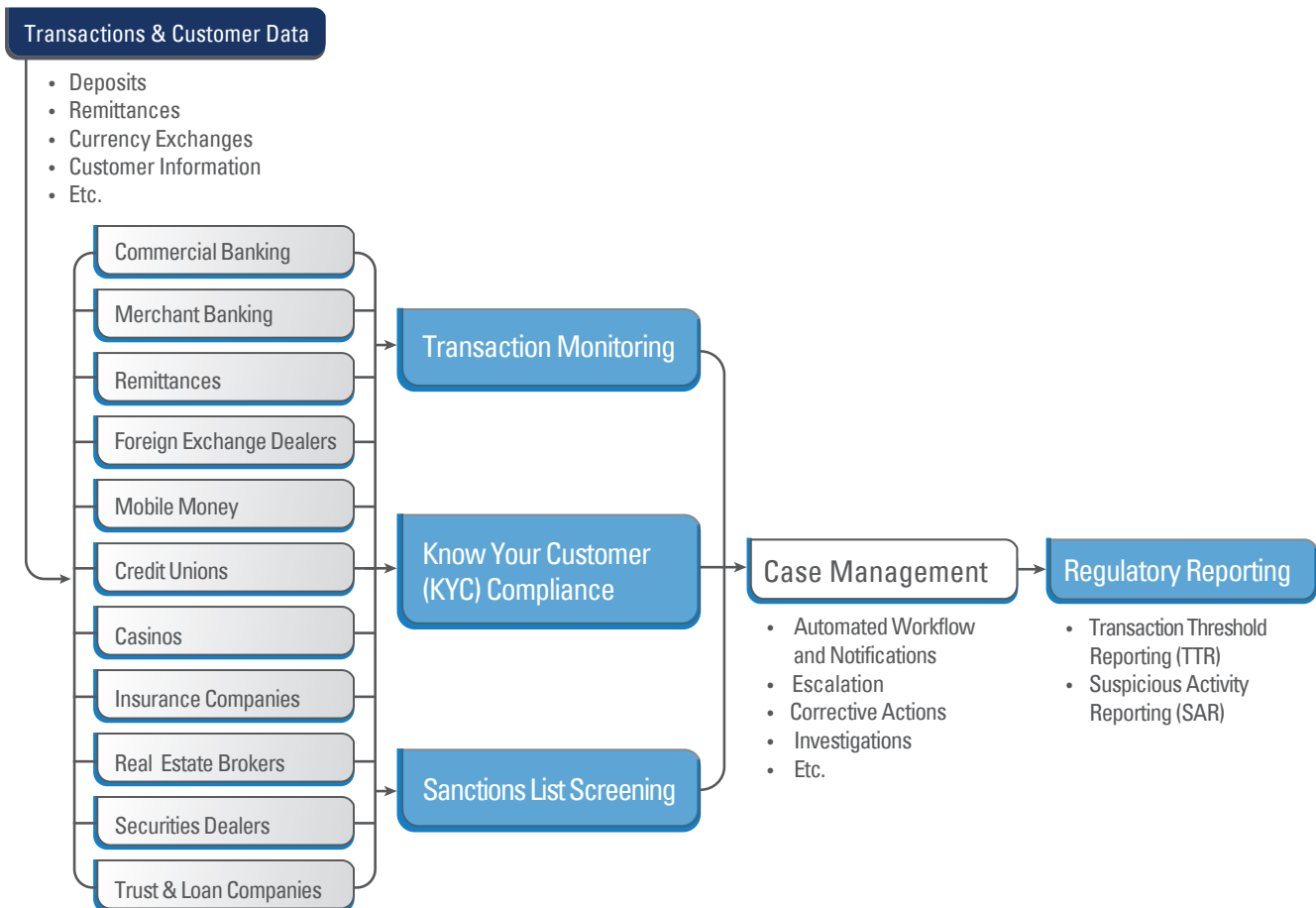
Solution Overview

Anti-Money Laundering Compliance

Cash lends to anonymity and is therefore a common medium of exchange for many forms of criminal activities such as drug and arms trafficking as well as fraud and corruption. The impact of these criminal activities globally have required countries to make concerted efforts to defend their institutions, financial systems, economies and citizens by criminalizing the proceeds of these illegal activities.

Compliance Programs and Intra-national Regulatory Requirements such as The Proceeds of Crime Act (POCA), The Bank Secrecy Act (BSA), Basel II, Sarbanes Oxley (SOX) and the USA Patriot Act dictate that financial institutions and their subsidiaries are required by law to integrate anti-money laundering measures into their operations.

Figure 1 - CaseWare™ Analytics AML Compliance Platform



CaseWare™ Analytics AML Compliance

CaseWare Analytics AML Compliance solution actively monitors 100% of financial transactions and customer information regardless of the banking application, ERP or CRM in use. The solution is able to assign responsibility for any non-compliant activity detected and maintain accurate records of all actions taken. This empowers institutions to take and evidence all the reasonable steps necessary, to exercise due diligence, to avoid committing an offence.

Transaction Monitoring

CaseWare's solution provides comprehensive coverage by monitoring all transactions across multiple locations or entities and any data source. Unique capabilities include:

- Cross-channel automated monitoring to detect and prevent anomalous behavior
- Consolidation of data from relevant sources such as Temenos, FIS™, Fiserv, Finacle, etc.
- Early identification of suspicious transactions including structuring, smurfing and flipping

Know Your Customer (KYC) Compliance

Verify your customers before doing business with them. You can now monitor your customers effectively by examining customer data to ensure KYC compliance and apply risk scores based on defined metrics.

Sanctions List Screening

CaseWare's solution allows you to screen individuals against sanction lists at various points in your process:

- ✓ **Onboarding** - While opening new accounts, screen potential customers and vendors
- ✓ **Periodic** - Screen your entire customer base on a regular basis to identify possible changes
- ✓ **During Transactions** – On a real-time basis, intercept transactions by screening senders and receivers of wire transfers and drafts
- ✓ **Thomson Reuters World-Check**

Used by 7,000 companies	800,000+ sources
PEP list of 900,000 names	Research in 240 countries

Regulatory Reporting

The solution automates the reporting process by allowing you to create and modify regulatory reports and capture notes and comments for reporting. You can report on suspicious activities and transactions that exceed defined thresholds in a timely and consistent manner.

CaseWare Analytics Capabilities

Workflow & Case Management

Perform enhanced due diligence to ensure non-compliant activities are properly investigated and reported. Through *automated notifications and workflow*, equipped with *time sensitive escalation* and *re-assignment features*, business stakeholders, can track and resolve exceptions in a collaborative manner.

Data Visualization for Risk, Controls & Compliance

Quickly determine if you're achieving your compliance objectives. Visualization dashboards provide insights into key performance indicators and help identify patterns and exceptions.

Identify and Resolve Data Quality Issues

Proactively discover data integrity issues before a compliance failure occurs and take the necessary steps to resolve issues across all entities.

AML Compliance Analytics

Transaction Monitoring	<ul style="list-style-type: none">○ Identify transactions by customer(s) exceeding a defined number of withdrawals or deposits over a specified period or across locations○ Identify all accounts closed with balances and any subsequent activity on those accounts○ Identify all cash withdrawals or deposits made at the ATM exceeding a defined tolerance○ Identify multiple cash deposit transactions that aggregate over the internal threshold
Know Your Customer Requirements	<ul style="list-style-type: none">○ Identify all customers without address data or with PO Box addresses only○ Identify potentially duplicated customers or customers with multiple, invalid or expired identification records○ Identify all customers with change of name and/or address○ Identify all accounts for which signing instructions have been amended○ Identify inactive accounts made active without the customer being made KYC compliant○ Identify inconsistencies in customer information across entities, etc.○ Identify related customers
Suspicious Activities	<ul style="list-style-type: none">○ Identify suspicious activity on accounts previously in a non-transaction state (such as Dormant/Inactive/Frozen)○ Identify High Risk Customers on new or joint accounts○ Identify significant informal relationships between customers

AML Compliance Analytics (continued)

Suspicious Activities (cont.)	<ul style="list-style-type: none">○ Identify corporate customers with cash transactions outside the normal course of business○ Identify sudden loan payments○ Identify ATM cards created and authorized by the same user○ Identify multiple ATM cards issued to the same customer○ Identify products that do not satisfy policy requirements (for example, interest rate, principal, term etc.)
Watchlist Searches	<ul style="list-style-type: none">○ Identify customers on Office of Foreign Assets Control (OFAC), Politically Exposed Persons (PEP) or Internal/Custom Lists
Remittances	<ul style="list-style-type: none">○ Identify remittances to and from blacklisted countries○ Identify instances of remittances to/from multiple recipients and/or senders exceeding a defined threshold○ Identify recipients consistently receiving money just below the threshold○ Identify suspicious transactions such as smurfing, flipping, etc.
Fund Transfers	<ul style="list-style-type: none">○ Identify customers sending or receiving wires to multiple persons that exceed or are just below the internal threshold○ Daily report on all incoming and outgoing wires and the sources○ Transfers from specific sources (reference established lists)○ Provide details of the source of funds information provided by customers
Staff Monitoring	<ul style="list-style-type: none">○ Identify transfer of funds from one staff account to another○ Identify all staff deposits, withdrawals, encashment of checks or fund transfers just within a predefined threshold○ Identify terminated employees still flagged as staff○ Identify users with access in violation of SoD○ Identify staff able to post their own transactions



469 King Street West, 2nd Floor
Toronto, Ontario M5V 1K4
1-800-265-4332 Ext: 2800
salesidea@caseware.com
www.casewareanalytics.com