PROTECT THE BANK
A New Approach to Fighting Financial Crime
Protect the Bank | Solution brief

Banks are feeling the growing burden of financial crime, which is putting a massive strain on bank resources and budgets. Sophisticated fraudsters continue to bypass and evade bank controls, and the continual release of new regulations from regulators in every jurisdiction makes compliance a permanently moving target.

With the move towards real-time payments and the acceleration of digital transformation to satisfy bank consumer demands for immediacy and personalization, banks have less time to monitor and take action, adding pressure to already overstretched compliance departments.

These factors are changing the way financial institutions fight financial crime. A siloed approach is no longer sufficient, as financial crime prevention now cuts across all corporate structures, processes and products, with many involved parties. An integrated financial crime platform is a necessity when it comes to effectively managing financial crime.
While each institution has its own selection of engines that perform checks and real-time monitoring of transaction flows, every bank has implemented these differently. In our experience, however, there are always some commonalities, namely that most of the operations are completed in silos throughout the bank.

Before we recommend how CGI’s Protect the Bank (PTB) solution can be applied and which components of the framework can quickly deliver benefits, a short consulting engagement is required to perform a current state assessment. This assessment is completed by industry experts located near the bank whenever possible.

PTB brings together a series of components, or digital enablers, into a framework that can be applied to any institution. Under normal circumstances, PTB does not require the wholesale replacement of core scanning engines or filtering solutions, but rather includes a series of enablers that are designed to make the existing infrastructure work better, faster and more accurately. Once implemented, PTB helps to reduce false positives across the institution, identify new types of fraud, and drive significant efficiency gains.
PTB is a single enterprise solution for addressing financial crime holistically across the organization. In delivering PTB, CGI works with our clients in one or more of these areas: strategic consulting, organizational change and program management, systems integration, solution implementation, managed services, and business process outsourcing.

CGI’s PTB framework integrates across bank silos to provide an effective financial crime management platform. The PTB framework can be applied independent of other solutions deployed at a bank. However, CGI also provides market-leading solutions that complement PTB, including: sanctions screening and know your customer (KYC) capabilities, both offered through CGI’s HotScan filtering software, suspicious activity monitoring with CENTaUR, fraud prevention with CGI ProperPay, and market abuse and transaction reporting through TTR360.

These solutions are brought together under a single command and control center, or case manager, where all alerts and notifications can be centrally managed, distributed, processed and monitored.

To drive the required efficiency gains, each component uses intelligent self-learning, which operates across traditional silos and with big data sources. Let’s now look at some of the core components and processes of PTB in more detail.
It is becoming increasingly difficult to reduce costs while trying to achieve tighter internal controls and improve anti-money laundering, fraud prevention and sanctions compliance. This is primarily due to the high volume of exceptions, the constant stream of complex new regulations, disconnected suspicious activity monitoring and fraud detection systems, and cumbersome manual processes. The implementation of strong technological controls is required to combat crime and provide a good audit trail.

CGI Case Management enables individual business areas within a bank to send all alerts to a single integrated case manager, which combines and manages all hits and notifications. Case Management acts as the command and control center for effective management of alerts, sanctions, fraud, suspicious activity and cyber crime.

The solution includes the following capabilities:
- Workflow automation (unlimited number of processes or business rules)
- Document management
- Communication (messaging, reminders, bring forwards)
- Status tracking
- Scheduling and calendaring (including automated scheduling or use of an interactive calendar)
- Reporting
- Configuration (allowing advanced business users to manage the information model)
- Business rules and workflow details of a business unit
- Role-based security model (providing customizable and personalized navigation menus based on user access rights)

The command and control center helps drive efficiencies and adds a new level of protection. As volumes grow, state-sponsored crime becomes more sophisticated, and more areas of the business move to real time, having a command and control center is an essential step for most financial institutions. Only by combining alerts in one system can banks identify multiple cyber attacks and spot sophisticated financial crime attacks across the business. This capability not only drives added protection, but also is at the heart of efficiency gains, which must be generated in order to support the move to real time.

Financial institutions are caught between their obligation to prevent illegal transactions and the rising costs of compliance. Robust sanctions screening can significantly reduce the time and cost required for sanctions compliance by analyzing all transactions and automatically alerting companies to potential matches against watch lists.

HotScan, CGI's award-winning sanction screening software, enables financial institutions to comply with international anti-money laundering regulations. It uses fuzzy matching techniques, manages multiple lists and jurisdictions, and works across both structured and unstructured data and data mining. HotScan searches out and finds references to people, companies and other entities with whom it is illegal to trade, or who have sanctions against them, or represent a heightened risk.

CGI's HotScan filtering software scales to scan all payments and customer data, provides notifications of matches against watch lists, and meets the constantly rising regulatory compliance bar. HotScan's industry-leading false positive reduction capability minimizes transaction delays and allows rapid and thorough review of customer data while reducing risks and operational costs.

HotScan employs the following:
- "Fuzzy matching" techniques, which are sophisticated algorithms for identifying sanctioned people and entities, despite accidental or deliberate misspellings that obscure their true identity
- Control of unstructured data and comparison with structured data
- Native language capabilities to scan and interpret all foreign alphabets, scripts and transliterations
- Algorithms that provide rapid, real-time data scanning
- Configurable scan settings and rules that enable fine-tuning to improve accuracy and achieve the organization's unique risk profile
HotScan also provides know your customer (KYC) capabilities. This includes real-time, ad-hoc screening due diligence, as well as batch screening for regular monthly customer account due diligence.

HotScan includes a politically exposed person (PEP) list module and integrated intelligent self-learning (ISL). By integrating ISL with KYC processes, a learning filter is applied, significantly reducing false positives and providing efficiency gains without narrowing the size of the net.

HotScan’s KYC capabilities provide many advantages, including the following:

- Increased productivity by reducing manual intervention and eliminating processing interruptions
- Minimized operational risks by achieving a balance between checking blocked accounts and maintaining continual transaction processing
- Implementation of risk assessments against terrorist lists, sanctioned entities, politically exposed people and other risk groups

- Reduced false positive alerts without negatively impacting the level of filtering, resulting in fewer manual checks, more effective compliance operations, and significant cost savings
Suspicious activity monitoring, which involves the analysis or investigation of unusual patterns of actions, is a major issue and covered by important regulations (e.g., The Bank Secrecy Act). It is based on the detection of agreed upon deviant cases sought by regulators or the police and is a good example of why flawed traditional approaches need to be modernized by minimizing silos and why different business processes need to be synergized.

By maintaining silos, grey zones occur and, just as importantly, synergies are wasted. The synergy benefits also impact functional units such as internal controls, compliance and investigation, risk management, and anti-fraud management. PTB drives both synergies and cost reduction.

Through CGI's suspicious activity monitoring solution, CENTaUR, an open modular platform is used to evaluate and analyze risks—monitoring account behavior across single and multiple channels using internal and external data. Pre-defined rules are used to detect suspicious (client or employee) activities and transactions.

CENTaUR features include the following:

- High-performance, scalable, real-time risk engine
- Integration interface through an adapter module
- Predictive analysis module that uses advanced statistical methods, visualization and modeling
- Data visualization and results of analytical processes
- Case management
- Reporting
- Analytical data warehouse (including profile and behavioral characteristic preparation)

Fraud

“Fraud” is defined in the Oxford dictionary as “wrongful or criminal deception intended to result in financial or personal gain.”

A “fraudster” is defined as “a person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities.”

These definitions show how wide the field is and how many components it contains. Fraud is a criminal human behavior. Soft skills and forensics are key elements to prevent a fraudster from being one step ahead.

CGI’s fraud solution CGI ProperPay helps financial institutions predict, prevent and protect against fraudulent acts. CGI ProperPay is configurable to an organization’s specific business rules. Its predictive analytics, workflow management, rules management and global best practices are available in the secure Microsoft Azure Cloud for even greater elasticity and power and include the following:

- Advanced algorithms to predict hidden patterns and anomalies within your data. Microsoft’s Cortana Analytics Suite is used to harness machine learning, perceptual intelligence and the cloud for predictive analytics. As models are exposed to new data, they incorporate this information to produce even more reliable, repeatable results.
- Analytics to prevent fraudulent activity and keep banking customers safer, allowing staff to easily identify patterns and audit data through a series of views and dashboards.
- Security to protect customer information. The Azure Cloud meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2.
- Technology to identify, stop and recover improper transactions to preserve bank revenue. Recovering a greater number of improper payments makes funds available to improve the customer experience. Business user-friendly features also free up valuable IT resources for other priorities.
Artificial intelligence (AI) and intelligent self-learning (ISL) are designed to deliver a very quick return on investment, helping institutions that need to deliver a controlled reduction in false positives. ISL is one of the most important requirements for any financial crime platform, allowing a feedback loop that improves filters by automatically discovering the good guys, thereby reducing the number of false positives and streamlining the review process. Further levels of AI can be introduced to improve other scanning and real-time processing areas.

CGI’s ISL module has been shown to reduce the number of false positives by up to 70%, without reducing the filtering accuracy or narrowing the net. It provides analysis of false positive history, discovery of good customers, and efficiency modeling.

Many institutions already use ISL-type solutions within their silos. However, with CGI’s PTB platform, ISL can be extended across all areas with access to big data sources. New algorithms can then be implemented to drive significant efficiency gains across different business areas and processes, improving effectiveness and overall protection. Fraud and sanctions systems effectively begin to talk to one another, sharing knowledge and results in real time.
In many cases, data (whether big or small) is somewhat unstructured (e.g., payment instructions, handwritten notes, disparate electronic lists, etc.), which can help facilitate financial crime. In addition to screening tools that can read and process unstructured data, having the ability to structure the data into a streamlined digital process is vital to managing the problem.

CGI can provide the required expertise, solutions and partnerships using our Data2Diamonds approach for simplifying data management and realizing value from analytics. This framework provides a blueprint for success in putting information to work. Our objectives are as follows:

- Shorten the “distance” between data assets and the people who need them
- Discover insights into important behaviors of people and machines
- Help clients use those insights to improve results

With more than 5,000 professionals devoted to business intelligence and information management, CGI offers the full range of business intelligence services for our clients, including consulting, integration of all major vendor applications, managed services and cloud-based, hosted systems.

In pilots already delivered, CGI has proven that, through the use of existing data feeds, big data can be used to spot new types of fraud based on the use of algorithms, which search for patterns, but are not based on rules. Over time, big data will be more integrated with artificial intelligence components and will help predict where fraud is coming from, even before it happens.

PTB uses the power of big data to provide additional levels of protection—uncovering and identifying areas of fraud, which until today often managed to bypass existing protection.
When looking at a bank’s sanctions violation, more often than not the violation was due to an insider threat who abused credentials or used stolen credentials to bypass the bank’s own processes. Sanctions violations have led to huge fines from regulators, damage to bank reputations and a significant negative impact on the bottom line.

At CGI, cyber protection and data privacy is embedded into what we do. To ensure protection of key processes and compliance areas within the bank, additional cyber controls and components may be needed to increase protection and help the bank identify insider threats before they do any damage. At CGI, we take a business-focused approach at every level—from audit and compliance to policy and architecture. Our end-to-end offerings include consulting and training, integration and implementation, managed services, and cyber insurance services.

PTB delivers a range of cyber protection components to enhance bank protection, particularly from insider threats, which are the most common and serious type of breach. We partner with our clients to assess and analyze potential cyber risks, continuously monitor for threats in real-time, put in place the necessary defenses, and ensure continuity of operations, even during a cyber incident.
Market abuse

While there is no substitute for real-time surveillance of a trading system as part of the control framework, regulators check through a mountain of data submitted to them under the guise of trade and transaction reporting. Until now, it has been the regulators who find discrepancies that point towards market manipulation and abuse and use shop windows to provide insight on how well (or not) a firm is meeting its responsibilities. This often leads to wider investigations.

Intelligent reporting systems head these issues off at the pass, not only by pre-validating reports but also through a swift and accurate triage to get to the root cause quickly. The PTB enabler for market abuse brings a single global reporting and management solution to institutions to provide protection both internally, as well as the necessary regulatory reporting in each jurisdiction.

Conclusion

Adopting an integrated approach to financial crime management helps to ensure the broadest possible coverage, improves return on risk and compliance investments, and enhances reputation.

With PTB, CGI offers a comprehensive, compliant approach to financial crime management, helping clients to implement smooth digital processes at reduced costs, while ensuring the institution is protected from financial crime.
About CGI

With more than 20 years of experience in developing and delivering cost-effective financial crime solutions, CGI’s 500+ compliance and security experts apply their deep understanding of the complex regulatory landscape to help leading organizations around the world fight financial crime.

CGI has been supporting and shaping the financial services market for nearly 40 years. We were behind the original design for the SWIFT interbank network and have worked with 70% of the world’s top financial institutions, including 8 of the top 10 global banks.

We work as a partner, not just a provider. Through a consistent, disciplined and accountable delivery approach, CGI has achieved an industry-leading track record of on time, within budget projects. As a result, our average client satisfaction score for the past 10 years has measured consistently higher than 9 out of 10. We are helping financial institutions, including most major banks and top insurers, reduce costs, increase efficiency and improve customer service.

© 2016 CGI GROUP INC.