rdc
Smarter Screening

PROTECTIVE SCRUTINY

The Role of Customer Screening in the Modern Customer Identification Program

THE QUEST FOR TRANSPARENCY

In our paper Financial Crime: Can We Win the War?, we covered how post-9/11 regulations, especially the USA PATRIOT Act, require banks and financial institutions to have a formal customer identification program (CIP) as part of their Bank Secrecy Act (BSA) compliance. The objective is full transparency and insight into each customer: their identify, their background, and the origin and nature of their funds. With this information, financial institutions are better prepared to identify potential financial criminals and prevent infiltration into their portfolio.

Some aspects of a CIP are fixed, while others have room for interpretation. The more an institution knows about the nuances of CIPs, the better able it is to protect itself against financial crime and stay compliant.

CIP Basics

Identity verification (IDV) is the fixed part of a CIP, enabling banks to obtain a clear and objective answer to the question: "Are you who you claim you are"? Anyone who has opened a traditional banking or investment account will be familiar with this process, in which we are asked to supply proof of identity such as a driver's license, passport or other government-issued identity card or number.

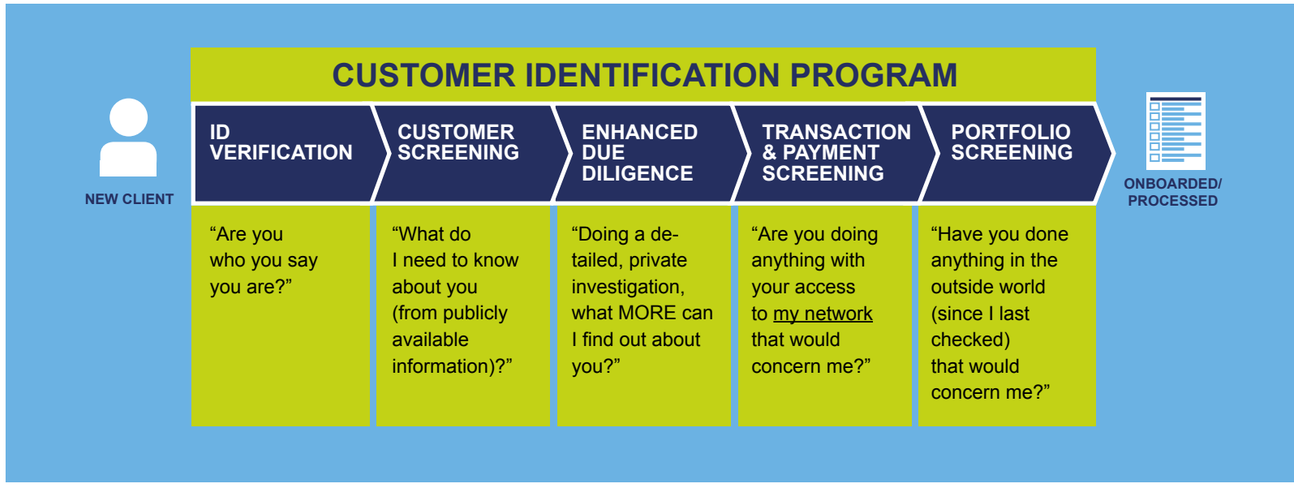
A second element of all CIPs is the ability to determine whether a customer appears on any federal government list of known or suspected terrorists or terrorist organizations. This is generally referred to as "Sanctions and Watchlist Screening", and the most frequently mentioned list is "OFAC Sanctions". This is published by the US Treasury Department's Office of Foreign Assets Control ("OFAC"), which enforces economic and trade sanctions against targeted foreign countries, regimes and individuals that are seen to pose a threat to the United States[1].

"CIPs NEED TO CONSTANTLY EVOLVE"

Beyond the Basic CIP

Most banks and financial institutions use more sophisticated CIPs that go beyond simple IDV and OFAC watchlist screening. Because financial crime is constantly evolving, CIPs need to constantly change and improve. BSA regulations also encourage more thorough CIPs, stating that "based on its risk assessment, a bank may require identifying information in addition to the items above for certain customers or product lines."

Today, most financial organizations have adopted a multi-step customer identification program similar to the process shown below.



It begins with identity verification, which establishes a customer's identity but does not show whether they are a potential criminal or what level of risk they present to the bank. To find that out, financial organizations use customer screening capabilities that leverage both public and often private information to determine the riskiness of the customer. Once a customer is onboarded, firms use a combination of payment screening and transaction monitoring to keep an eye on the flow of money, trying to spot potential sources or destinations of illegal funds. They may also use periodic re-screening to address the fact that a low-risk customer isn't necessarily low-risk for life.

For the purposes of this paper, we want to focus on customer screening and the role it plays in the overall customer identification process.

Technology-driven customer screening has become a powerful weapon in the battle against financial crime, helping organizations to:

- Identify the "riskiness" of a customer.
- Accelerate onboarding of low-risk customers.
- Focus on higher-risk customers. Banks may elect to perform additional research on the customer, usually referred to as "enhanced due diligence" or EDD.
- Screen their entire portfolio on a continuous basis to pick up customers that may appear to be low-risk at first but could engage in criminal activities later.
- Reduce the need for huge teams of Level 1 analysts to manually screen customer account information, instead deploying those resources to more valuable efforts.

Source

[1] *https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx*

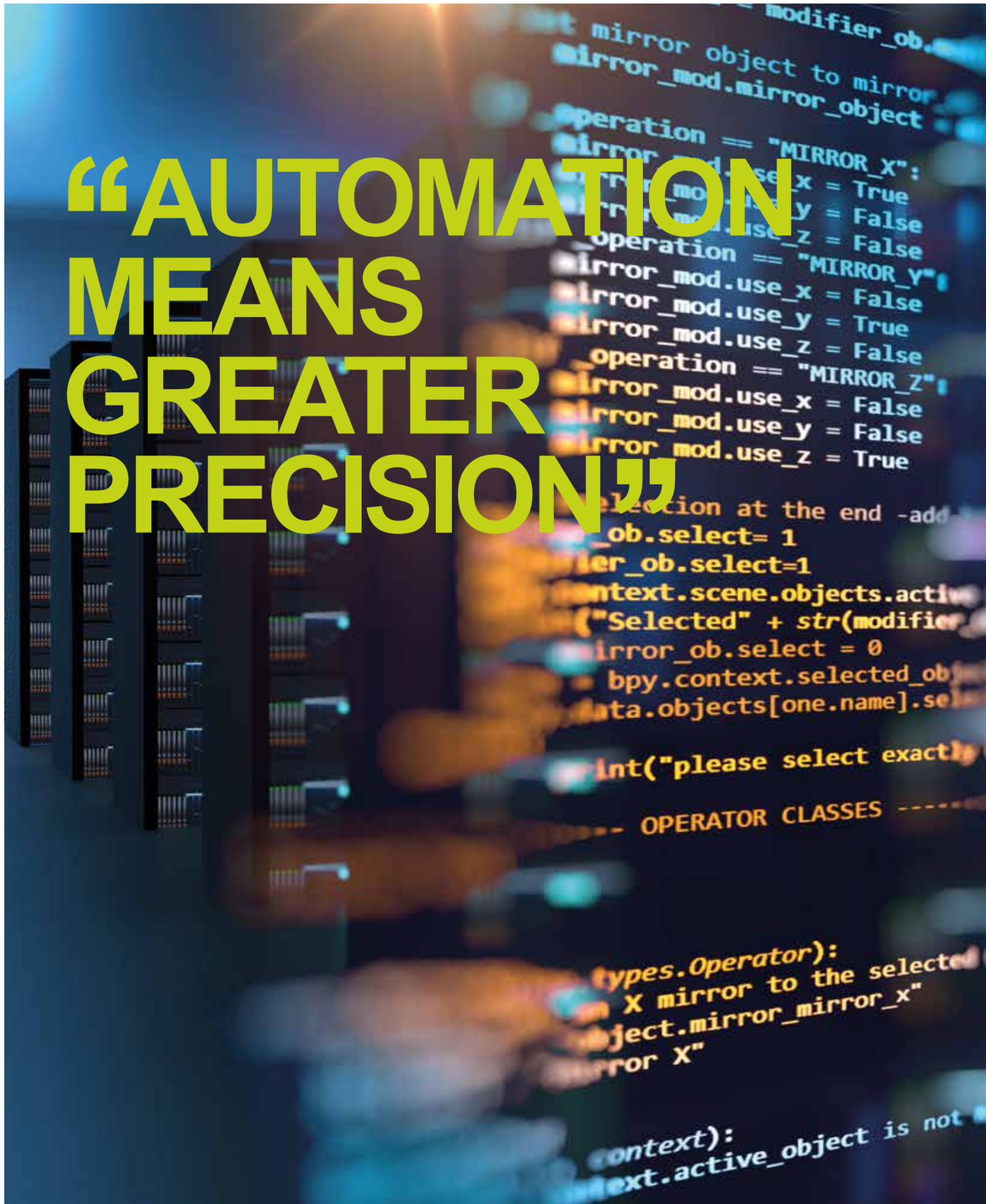
How Customer Screening Varies

Given the value of customer screening, it's no surprise that financial institutions continue to invest heavily in their capabilities. However, every organization approaches it differently. Here are some of the variations and tradeoffs that we frequently see in the market:

- **Sanctions & Watchlists.** Some banks screen against basic government sanctions lists while others screen against a much wider array of watchlists. Providing potentially valuable insights, these additional lists can include: regulatory agencies' actions, fugitive lists, exclusions lists, fraud warnings, debarment lists, disciplinary actions, enforcement actions and the law enforcement press.
- **Politically Exposed Persons (PEPs).** Virtually every bank needs to determine whether the customer is, or is closely related or associated with a PEP – an individual entrusted with a prominent public function. PEPs present a higher risk for bribery and corruption by virtue of their position and influence. Some banks screen solely against limited sets of PEPs (e.g. country and state leaders) while others widen the net to include PEPs such as judicial and military leaders.
- **Adverse Media.** Screening customers for negative mentions in public domain news and data sources can identify individuals who do feature on watchlists or are defined as PEPs. However, many organizations do not include Adverse Media in their screening program and choose to simply rely on PEPs and Sanctions/Watchlist screening.

- **Variation by Region.** Some global financial institutions have regional customer screening centers, with the focus on keeping the screening closest to the customers. Other organizations have moved to a center-of-excellence or "COE" model to gain greater consistency, efficiencies and cost savings.
- **Variation by Lines of Business.** Large global financial institutions have a variety of business units including commercial banking, retail banking, mortgage, private wealth management, real estate, investment banking, to name a few. Some choose a common screening approach across all lines of business while others tailor it to the needs of the specific business unit.
- **Manual vs. Automated.** Even though volume and complexity of financial crime has changed considerably over the past 5-10 years, many financial organizations still lean heavily on a manual approach. Vast teams of compliance analysts are tasked with researching each customer, often relying on search engines and similar tools to determine the riskiness of an individual. Increasingly, organizations are turning to more automated, intelligence-driven solutions that can help analysts screen customers faster and with greater precision.

- **On-Premise vs. Cloud.** Financial institutions that opt for a technology-based screening solution need to determine whether to move forward with an on-premise solution (that operates behind the company's firewall) or a cloud-based solution (that operates on a secure cloud platform such as Amazon Web Services).



THE ROUTE TO SUPERIOR SCREENING

Customer screening is a vital and often under-appreciated component of a high-performance customer identification program (CIP), itself a critical weapon in the fight against financial crime. While ID verification remains an important starting point for any CIP program, it is customer screening that truly addresses the issue of the riskiness of the customer, both during onboarding and on a continuing basis.

What's important is to choose the balance of screening activity that responds to both regulatory demands and the risk profile of your organization.

With a comprehensive screening program that incorporates sanctions, watchlists, PEPs and Adverse Media, organizations get a much richer, contextual perspective into the current and potential risk of a customer. With this deeper data set, you can implement a risk-based program tailored for specific regions or lines of business rather than "one-size-fits-all" approach that may miss critical risks. Based on our experience from nearly 1,000 customers and 20 years of screening results, this approach delivers superior screening outcomes, greater operating efficiency and can reduce the overall costs of compliance.

rdc
Smarter Screening

Discover more
rdc.com