Identify and Prevent Financial Crime Schemes Arising from Current Pandemic Circumstances

In a New Global Pandemic Era, Stay One Step Ahead of Today's Financial Criminals

Financial criminals, money launderers, and fraudsters cause serious trouble for financial institutions in the best of times. During a global pandemic, the opportunities to wreak havoc, and the extent of the damage these criminals can inflict, are magnified tenfold. As early as March 2020—the same month the World Health Organization declared the worldwide crisis—COVID-19-related financial crimes were already increasing exponentially. And they haven't abated since.

In response, international standards and national regulatory bodies have upped their expectations and have put the onus on financial institutions to enact stricter anti-money laundering measures. Specifically, these regulations require financial institutions (FIs) to be on the lookout for a wide range of emerging money laundering and fraud schemes orchestrated to exploit the COVID-19 situation.

Let EastNets do the legwork to help you protect your financial institution and your customers.

The anti-money laundering and counter terrorist financing (AML/CTF) experts at EastNets have put substantial time and effort into interpreting regulatory requirements, identifying the increasing risks and red flags, and understanding evolving financial crime schemes in play today.

Our team has translated volumes of information into a comprehensive list of more than 20 new scenarios and typologies related to COVID-19 that you can put to work right away to enhance your institution's approach to risk-based behavior and transaction monitoring during the pandemic.

COMPLIANCE SOLUTIONS

UPDATE YOUR AML SECURITY FOR THE COVID-19 ERA

With COVID-19 Financial Crime Monitoring from EastNets, your institution can:

- Enjoy greater protection against more than 20 types of emerging financial crime schemes related to COVID-19.
- Save time and resources with ready-to-use scenarios and professional rule configuration and implementation by the EastNets experts.
- Maintain a low false positive rate with well-defined rules and high operational efficiencies.

We've built specific customer, account, and entity scenarios to pinpoint and prioritize suspicious activity with a minimum of false positives, so you can protect your customers and assets without creating unnecessary work for your team.
With EastNets updated COVID-19 Financial Crime Monitoring, you can trust our team to integrate these new scenarios into your new or existing EastNets financial crime solutions. We expertly configure the rules and analytics capabilities and define the logic so you can quickly, easily, and confidently begin defending against today's most disruptive financial crimes.

Identify threats in 9 major COVID-specific categories.

When the EastNets team helps you deploy COVID-19 Financial Crime Monitoring, your institution will be ready to automatically identify suspicious behaviors and payment transactions related to more than 20 new scenarios of fraud and AML schemes in the following key areas:

Financial Assistance Monitoring

With an increase in national stimulus programs geared toward both individuals and businesses, criminals are increasingly filing fraudulent claims and falsely qualifying for assistance. Rules are set and deployed to look for deviations in transaction behavior and other patterns that are indicative of this type of fraud.

COMPLIANCE SOLUTIONS

- Comply with the latest anti-money laundering rules, regulations, and reporting requirements from entities including FATF International Standards, FinCEN, UN resolutions, the EU anti-money laundering directive (AMLD), and the U.S. Patriot Act.
- Avoid penalties and fines associated with inadequate financial controls.
- Quickly and seamlessly upgrade your existing AML/CTF solutions, including en.SafeWatch Profiling®, en.SafeWatch Filtering®, and en.SafeTrade.

Specific Customer Monitoring

The elderly, children, and non-profit organizations are some of the most vulnerable to emerging COVID-19 financial scams. Adding new monitoring scenarios specific to these populations and entities, as well as taking a closer look at the behaviors of government officials and politically exposed persons (PEPs), can help pinpoint some of the major types of emerging corruption and fraud.

Traditional Transactions Monitoring

With online transactions on the rise during the pandemic, other types of transactions should decrease accordingly. When they don't, it could be a sign of trouble. By ferreting out these situations, financial institutions can quickly pinpoint and intercept potential criminal activity.

Cards Transactions Monitoring

With many businesses closed during the pandemic and travel restricted, credit card or ATM transactions made during lockdown hours or in foreign countries—especially on cards that have never been used in those countries before—are major red flags. To thwart such red flags, new scenarios pay specific attention to transactions in high-risk countries and those most impacted by COVID-19 as well as to entities subjected to lockdowns.

Security Market Industry Monitoring

Customers working in certain industries have the opportunity to capitalize on the pandemic by engaging in insider-trading. Monitoring for an unusual amount or frequency of such transactions can tip off financial institutions to potential bad actors.

Fund Transfer Transaction Monitoring

Banks should check for unusual incoming or outcoming wire transfers, especially cross-border transactions or those involving high-risk countries or countries disproportionally affected by the pandemic. An unusual frequency of wire transfers or those from or to inactive, new, or dormant accounts or accounts with no previous history of wire transfers also deserve a closer look.

Affected Businesses and Professions Monitoring

Criminals often use front businesses to launder money. Right now, many of those businesses are closed or operating at a much lower volume than usual. It's a good idea to keep an eye on the activity of restaurants, pubs, hotels, lawyers, beauty centers, car dealers, and businesses in similar industries for signs of transactions occurring while the organizations are supposedly locked down.

Trade-Related Transactions Monitoring

During COVID, some criminals are using the high demand and limited availability of medical supplies to send fraudulent requests for advanced payment on goods they never have the intention of delivering. Signs of this type of scam include trading with countries hard-hit by the pandemic, trading with new counterparties, and trading with beneficiaries who are not active in the distribution of COVID-19 materials. Transaction messages should also be monitored for content with specific keywords, such as COVID-19, Coronavirus, SARS-CoV-2, Masque, or Mask.

Deposit Monitoring

Cancellation of major purchases is increasing during the pandemic, giving criminals the opportunity to deposit illicit funds and claim the money came from a refund on a legitimate purchase, such as a property, car, furniture, business, or holiday. Any extremely large deposits as well as deposits that deviate from declared activities should arose suspicion and justify a second look. monitored for content with specific keywords, such as COVID-19, Coronavirus, SARS-CoV-2, Masque, or Mask.

For more information on COVID-19 Financial Crimes Monitoring or to see how it works in conjunction with EastNets proven AML/CTF solutions, contact EastNets today.

CONTACT US

info@eastnets.com
www.eastnets.com

EastNets®
financial integrity. delivered.