

# Find the Activity, Stop the Money, Slow the Crime

---

Use Advanced Analytics to Flag the  
Warning Signs of Predicate Crime

---

Financial institutions are under increasing regulatory pressure to monitor transaction and account activity for indicators of predicate crimes (That is, illicit activities that funnel money into money laundering channels). By recognizing and reporting suspicious activities, parties and protocols, financial institutions can help to mitigate this illicit activity and save its potential victims from harm.

---

Detecting such predicate crime indicators – often different from downstream money laundering indicators – can be complicated. Advanced detection and analysis technologies can reduce the burden on compliance staff and improve the effectiveness of such efforts.

The Financial Crimes Enforcement Network (FinCEN) identifies four types of predicate crime on the rise, with examples of the indicators to watch for.

## Human Trafficking

Human traffickers coerce or force vulnerable individuals into labor or commercial sex acts in a variety of locations and industries. FinCEN notes that human trafficking is a highly profitable international crime, generating about \$150 billion annually worldwide. The COVID-19 pandemic has exacerbated the conditions that contribute to human trafficking, including weakened support structures.

The Bank Secrecy Act (BSA) identifies several methods that human traffickers use to launder proceeds, including front companies, funnel accounts and the use of alternative payment methods. Financial institutions should look for these warning signs:

- Transactions that are inconsistent with expected activity, involve foreign online classified sites or use third-party payment processors that conceal originators or beneficiaries
- Frequent cash deposits with no Automated Clearing House (ACH) payments
- Excessive purchase or use of prepaid access cards or cryptocurrency
- Third parties speaking on behalf of or acting in an aggressive or intimidating way toward the accountholder

A [FinCEN advisory](#) provides more information on identifying and reporting human trafficking and related activity.

## Environmental Crimes

As the third largest illicit activity globally, environmental crimes produce hundreds of billions of dollars in illicit proceeds each year and are growing at a rate of 5% or more per year. Wildlife, waste and hazardous-substance trafficking, as well as illegal logging and mining, harm human health, damage environmental quality, create biodiversity loss and overexploit natural resources.

Because enforcement efforts and penalties are limited and demand is high, these crimes are considered low risk and high reward.

Warning signs for specific activities include:

- **Illicit wildlife trafficking:** Can be facilitated by several funding mechanisms, including cash; bank transfers (wires and ACH); transfers through informal values transfer systems; transfers through money services businesses; transfers conducted using online or mobile payment processors; and transactions using convertible virtual currencies (CVC)
- **Illegal logging and mining:** Commingled with legal trade, this illicit trade may involve corporate structures, the use of shell companies in various jurisdictions and the movement of proceeds in the international financial system
- **Waste and hazardous substance trafficking:** May involve purchases of companies by persons lacking adequate knowledge and experience in the waste sector to manage entities operating in a highly regulated sector; high volume/value of cash deposits and withdrawals by waste management sector companies; large international funds transfer between local waste management sector companies and known major importer/destination for waste trafficking

Read FinCEN's [advisory](#) to learn more about detecting financial activity related to environmental crime.

## Ransomware

Ransomware is malware that blocks access to a computer system or data, often through encryption, in an attempt to extort ransom payments. Perpetrators might also threaten to publish sensitive data. Such attacks have increased rapidly over the past few years and include the May 2021 attack against Colonial Pipeline, the largest pipeline system for refined oil products in the United States. Targets include the government, infrastructure, manufacturing, legal services, insurance, financial services, healthcare, energy and food production sectors.

Financial institutions should watch for these indicators of ransomware-related activity:

- Irregular transactions between an organization especially one from a high-risk sector – and a digital forensic and incident response or cyber insurance company known to facilitate ransomware payments
- The sudden purchase or transmission of large CVC transactions, especially outside an account's normal business practices
- Accountholders' use of a foreign-located CVC exchanger in a high-risk jurisdiction
- Receipt of a CVC from an external wallet, immediately followed by multiple trades across multiple CVCs or anonymity-enhanced cryptocurrencies (AEC) with no apparent-related purpose and a final transaction off the platform
- Accountholders who initiate a transfer of funds involving a CVC mixing service
- Accountholder use of an encrypted network or unidentified web portal to communicate with the recipient of a CVC transaction

For more information about ransomware and how criminals use the financial system to facilitate ransom payments, see FinCEN's published [advisory](#).

## Economic Impact Payment (EIP) Fraud

EIPs authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act or Coronavirus Response and Relief Supplemental Appropriations Act of 2021 have been targeted in a range of frauds and thefts, including altered or counterfeit checks, phishing schemes and inappropriate seizure of funds. Red flags include the following:

- An attempt to deposit one or more fraudulent or counterfeit checks that appear to be issued by the U.S. Treasury, or receipt of an excessive number of EIP deposits linked to the same address
- Multiple EIP-related deposits for individuals other than the accountholder, or individuals outside the accountholder's geographic region
- Deposit of EIP funds into dormant accounts with little or no prior activity
- Rapid transfer of multiple EIPs into one account, followed by large cash withdrawals or serial ATM withdrawals; purchase of CVCs or prepaid debit or gift cards; transfer through a money services business or wire transfer; or large purchases at merchants that offer cash back as an option
- Deposits of EIP checks or electronic deposits into an account held by a retail business or a personal account of a business owner or employee that is not the payee or endorser
- Use of the same IP address, especially one located outside the U.S., to transfer funds from several EIP debit cards to one account
- Numerous deposits or EFTs that indicate the payments are linked to EIPs or unemployment insurance payments from one or more states in names that do not match the accountholders

For more information, see the [FinCEN advisory](#) on financial crimes targeting COVID-19 economic impact payments.

## How Technology Can Help

Transactions involving these illicit activities can form the basis for federal criminal charges, so the ability to create scenarios to identify red flags is vital. No one indicator is typically sufficient to prove wrongdoing, but the flags discussed here, among others, can alert compliance staff to the need for further investigation.

Recognizing illicit financial activities can be complicated and time consuming. Analysts can benefit from the use of enhanced analytics, machine learning, and data science to create specific scenarios and optimize resources to focus on high-risk alerts.


Accurate data plays an important role in successful machine learning and analytics. The automated funneling and filtering of data enables the development of behavioral profiles. These profiles, based on machine learning identification of specific behavioral patterns, can point to the warning signs of financial crime. Once informed scenario models are created from the profiles, the process can flow automatically. Data is ingested and cleansed, then given a risk score. Based on an institution's risk threshold, scores can be ranked and prioritized accordingly.

Enhanced software tools can automatically send the most urgent alerts to analysts for immediate review. Analysts can easily see critical information they need to perform a holistic analysis and make quick, accurate decisions.




# Connect With Us

For more information about  
Financial Crime Risk Management:

 800-872-7882

 getsolutions@fiserv.com

 [fiserv.com](https://www.fiserv.com)

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today.

Visit [fiserv.com](https://www.fiserv.com) to learn more.