

# Emerging Financial Crime Risks and Strategies for Financial Institutions

---

Responsive and Effective  
Measures to Fight a New Wave of  
Criminal Activity

---

**Financial crime is growing even as costs for compliance and detection soar. The imbalance of investment and efficacy send a message: Meeting compliance requirements is important, but more needs to be done to attack the problem. Instead of checking boxes, financial institutions may want to pursue actions that have more material impact on the amount of money that's laundered through the financial system.**

---



U.S. and Canadian financial firms spent a projected \$42 billion on financial crime compliance in 2020 – a 33 percent increase over 2019, according to True Cost of Financial Crime Compliance, a 2020 report by LexisNexis. Despite that investment, money laundering detection statistics have barely improved. Year after year, the United Nations' Office on Drug and Crimes estimates that 2 to 5 percent of global GDP moves through the financial system illegally – and less than 0.2 percent of that amount is detected.

Money laundering comes with a bigger price tag than what's spent on compliance. It empowers terrorist activities and crimes against humanity, including human trafficking, vulnerable adult abuse and wildlife trade.

Money laundering is not a victimless crime and there is a higher risk of exploitation during times of crisis and economic distress, such as the COVID-19 pandemic. Organized criminals have clearly taken advantage of the current situation. According to the Federal Trade Commission (FTC), [U.S. consumers lost more than \\$3.3 billion to fraud in 2020](#), up from \$1.8 billion in 2019. And reports of identity theft received through the FTC nearly doubled in the U.S. in 2020.

New financial crime data from the FTC, as well as strategic initiatives coming out of the Financial Action Task Force (FATF), the European Commission and other legislative bodies point to several areas of exposure and emerging risk. For financial institutions, protecting their organizations and the communities they serve means focusing on the following priorities.

## Cybercrime

In-person banking activities abruptly stopped during the pandemic, shifting more traffic and attention on digital channels. Criminals took advantage of the accelerated change and the physical distance separating consumers from their financial institutions.

The pandemic fueled a resurgence in synthetic identity fraud, a crime in which fraudsters use a mash-up of real (typically stolen) and fake information to create a new identity. The fraudulent identity is then used to open accounts. By some measures, synthetic identity is the fastest-growing financial crime. Victims of this type of fraud are typically the most vulnerable populations – children, the elderly and people who are homeless.

Electronic know-your-customer (KYC) strategies can help financial organizations respond to emerging risks. Consumers should be onboarded and served safely from any location without detracting from the consumer experience. That requires new protocols for due diligence and what constitutes sufficient identification to establish a customer relationship. Collaboration between IT and anti-money laundering (AML) teams can help protect consumer information accessed from off-site work locations, such as an employee's home office.

## Predicate Crimes

The European Union recently expanded the scope of money laundering, giving financial institutions more responsibility and power to combat predicate offenses, which are components of larger crimes. Money laundering that aids or abets criminal activity is considered legally culpable under the EU's [Sixth Anti-Money Laundering Directive](#).

As such, inspections are increasingly focused on predicate offenses. Regulators want to know how financial institutions are implementing local laws and mitigating specific crimes against humanity.

That changes how financial institutions think about money laundering, widening the perspective to include more suspicious activities, parties and protocols. Red flags for predicate crime may be different than downstream money laundering. Financial institutions need to be aware of schemes, so they can apply the right technologies and processes to identify criminal activity – even if it's primarily nonfinancial.



### Catching Criminals: Red Flags for Financial Crime

The FATF issued guidance to help financial institutions detect suspicious activity. It suggests creating internal controls and financial crime indicators to catch these red flags for criminal activity:



### Bribery and Corruption

- Unusual disbursements, deposits or standing order activity
- Investment or receipt of funds exceeds normal value for income or occupation
- Transactions to or from a new counterparty
- Large transactions in flagged areas (for example, luxury goods, dividends and so on)
- International transfers or unusual payments to or from politically exposed persons



## Abuse of Vulnerable People

- Products or services inconsistent with a client's risk appetite or profile
- Portfolio changes after initiating a power of attorney
- Requests that indicate the policy/ account holder is traveling or unreachable
- Use of email accounts that don't require personal information or verification
- An unusual number of account contact changes followed by an outflow of funds
- Loan requests that occur shortly after online product registration or an address change
- Requests to transfer loans to an account, address or post office box that is not on the bank account or address of record



## Market Abuse and Sales Malpractice

- Advisors who have the same address as their clients or who have many clients at the same address
- Advisors whose clients are missing date of birth or address information
- Above average number of accounts per client or number of accounts with face reductions
- Below average account persistency



## Human Trafficking

- Transactions and balances that are inconsistent with a stated business or job, or funds received are above a stated income
- Addresses and phone numbers are detected on classified websites
- Prepaid cards are used to purchase travel or hotel stays in multiple cities in a short timeframe
- Transactions that match certain key words (for example, massage, adult or household services)
- ATM and credit card charges outside normal operating hours



## Collaboration

There's a stronger global appetite for coordination and information sharing between financial institutions and regulatory and enforcement agencies.

Very early in the pandemic, Australia, Italy and Singapore started publishing scam alerts to inform and protect the public. Regulators in those countries offered greater latitude on timing, so financial institutions could focus on customers' needs and risks. The FATF published prescriptive guidance and red flags for financial institutions to watch for.

Together, regulators and financial institutions learned how to effectively manage remote examinations. To achieve better outcomes, collaboration and a laser focus on efficacy will need to continue after the pandemic.

## Supportive Infrastructure

New collaborations and measures to fight financial crime are important but cannot be realized without supporting systems, processes and people.

For example, in the U.S., the [Anti-Money Laundering Act of 2020](#) announced a new beneficial ownership registry within the Treasury Department's Financial Crimes Enforcement Network. The database will improve transparency and give U.S. law enforcement agencies a boost over organized crime and individuals who finance criminal activities through shell companies and other illicit means.

While the new registry will absorb some of the reporting burden for financial institutions, it does not absolve organizations from performing all due diligence and KYC requirements. Financial institutions need to carefully ensure their AML practices remain compliant with updated regulations.

The Anti-Money Laundering Act also issued new whistleblower incentives and protections. Organizations will need to give their employees mechanisms to identify red flags and to pass information back to the compliance function or to law enforcement.

And with Brexit, there are new definitions of sanctioned parties. Wherever they are, UK citizens and entities that are incorporated under UK law must comply with sanction requirements. To comply, companies need to have controls in place to help them identify their employees' nationalities and places of residence.

## Empowering People

There are many ways to apply technology to deter financial crime. But the human element cannot be ignored as a powerful force for combatting malicious activity. The right people need the right training to maximize effectiveness and realize the potential of digital tools.

People need to use AML collectively – using information from throughout the organization. They also need to use AML smartly by asking the right questions of the right data. When used correctly, AML technologies serve as an enabler and a connector. Ultimately, staff members' curiosity and dedication will guide the technology and help uncover new risks and vulnerabilities.

## Maximizing Effectiveness


All of these trends and changes point to one reality: Financial institutions need more responsive and effective measures to fight criminal activity – not just financial crime.

Financial institutions are in a unique position to affect and improve lives, especially those being exploited by organized criminals. By working collaboratively in their organizations and across regulatory and law enforcement agencies, the industry can achieve greater efficacy.

Tools, people and processes must come together to protect vulnerable populations and the global financial system.

# Connect With Us

For more information  
about AML Risk Manager:

 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.