IDC

SPOTLIGHT

Sponsored by: TaskUs

U.S. financial institutions face complex regulatory compliance to deal with an increasing wave of fraud and financial crime. Banks and credit unions can seek solutions from trusted compliance partners that use human assessment and AI tools to fight financial fraud.

Using Compliance Services Solutions to Counteract Bank Fraud and Financial Crime

January 2025

Written by: Raymond Pucci, Research Director, Intelligent Finance and Customer Care Business Process Services

Introduction

Bank fraud and related financial crimes threaten account holders and the banking system. They challenge financial institutions (FIs) to develop effective fraud management systems while managing their operations. Fraudsters are continually refining their methods to open fake accounts or launder money to sustain their illegal activities. The latest tactics, such as synthetic fraud that uses actual personal identities, and cryptocurrency-related schemes are more difficult to detect and prevent. This increases the urgency for FIs to use highly effective AI-based, anti-fraud solutions with collaborative human oversight. A 2024 Nasdaq study, Global Financial Crimes Report, finds that financial fraud and crimes across the globe cost billions of dollars annually. The report states that in 2023, money laundering and illicit funds flowing in the United States totaled $845 billion. For the same year, the study estimates consumer and business fraud to be $138 billion, including $127 billion related to fraudulent transactions in payments, checking accounts, and credit cards (see Figure 1).

AT A GLANCE

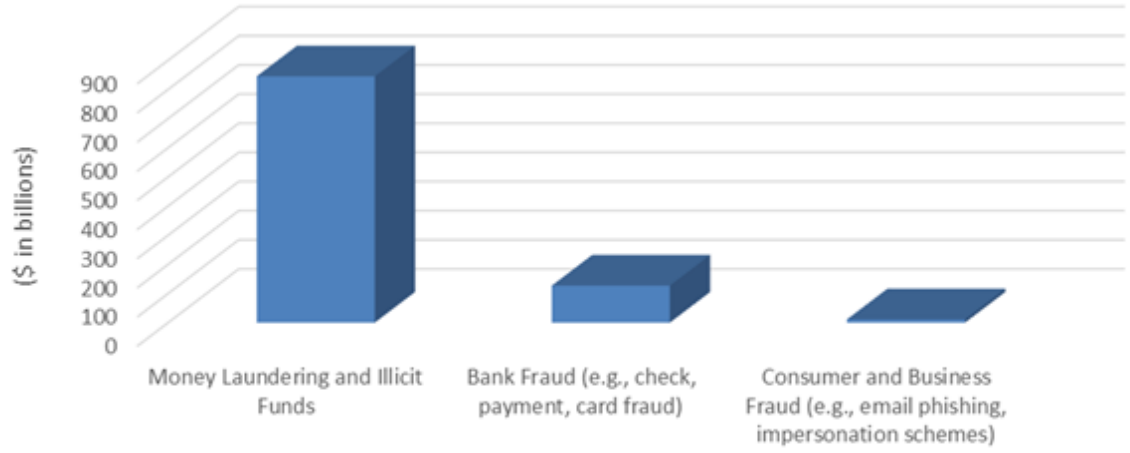
KEY TAKEAWAY

Bank fraud and financial crime in the United States remain high, impacting financial institutions and their customers. Banks and credit unions must maintain strong due diligence processes with assistance from technology partners to remain compliant with and avoid penalties from multilayered government regulators.

WHAT'S IMPORTANT

AI-integrated fraud management programs are essential to counteract financial crime while protecting financial assets and preserving customer trust. Emerging technology trends include GenAI solutions that will significantly enhance fraud detection and accelerate credit decisions by lenders.

FIGURE 1: ***Estimated Financial Crime and Fraud Losses for the United States in 2023***



Source: Nasdaq's Global Financial Crime Report, 2024

Operationalizing Fraud Management While Servicing Customers

Digital commerce presents both opportunities and challenges for the financial services industry and its major segments of banks and credit unions. Through the digitization of customer delivery channels, these FIs have expanded their reach by opening new customer accounts and creating cross-selling opportunities. Whether onboarding new accounts or assessing loan applications, FIs must increase their vigilance against fraud and related financial crimes. The expanding virtual nature of digital banking means increased security threats, such as identity fraud, money laundering, and illegal financial activity. Although digital platforms bring operational benefits and strategic advantages for banks and credit unions and enhance customer experiences, they also result in increased risk and security issues from fraudsters and their illicit trade. An overlapping, multilayered system of federal and state government agencies mandates that financial institutions comply with fraud prevention and risk management regulations to protect financial systems and consumer and business account holders. FIs must adhere to all financial industry laws and regulations. Failing to do so results in fines, sanctions, and reputational damage.

Financial institutions must continually improve their anti-fraud measures to counteract savvy fraudsters. Successful risk management and fraud prevention programs typically utilize a combination of human processes and technology applications to thwart financial criminals. This hybrid approach ensures that financial institutions can proactively identify and prevent future fraud while meeting the compliance regulations of government overseers.

Account Origination Requires Due Diligence

While fraudsters have various access vectors into financial institutions, a key entry point is account origination. Banks have increasingly struggled to counteract this, as online and digital access gives fraudsters anonymity and allows them to frequently use false synthetic identification. They use stolen identifiable identification points — such as Social Security numbers, addresses, and bank account data — from multiple individuals to create a fake digital application to open a checking account or apply for a loan. Key compliance requirements in the due diligence process include know your

customer (KYC) and know your business (KYB), which government regulators closely monitor in their fraud prevention and anti–money laundering efforts. Ineffective due diligence is one of the most frequent compliance violations and is a key reason FIs turn to technology partners that use AI and machine learning solutions to help manage the process.

Fraud Fallout Impacts Downstream Banking Services

Ineffective and error-prone fraud management programs adversely affect downstream banking services, such as loan decision-making and account opening, resulting in poor customer experiences. Further, inaccurate fraud prevention measures can mistake legitimate customers for fraudulent ones, denying them loans or online purchases. Financial institutions should conduct operation risk assessments and work with tech partners to choose the right level of risk-return rates to optimize revenue and retain adequate fraud protection for customer transactions.

U.S. Regulators Increasing Compliance Monitoring

Past bank failures and financial system shocks have spawned a myriad of banking and financial regulations that multiple government agencies enforce at both federal and state levels. An array of sometimes overlapping U.S. financial regulators includes the Federal Reserve Bank, Office of Comptroller of the Currency, Financial Deposit Insurance Corporation, Consumer Financial Protection Bureau, and the National Credit Union Administration, plus bank overseers across all 50 states. U.S. banking regulations cover various fraud and financial crime categories intended to protect the financial system, consumers, and businesses. Regulatory compliance and reporting demand complex and detailed procedures, requiring financial institutions to undertake highly systemized operational processes. Regulations cover various categories, including money laundering, terrorist watch lists, consumer protection, credit disclosure, and lending requirements. Key U.S. bank regulations include:

- **Bank Secrecy Act:** An anti–money laundering regulation that requires banks to report suspicious activity, high dollar transactions (over $10,000), and cash purchases of negotiable instruments
- **Patriot Act:** A requirement for increased KYC/KYB verification and sharing of account information among financial institutions to report possible illegal transactions and activities
- **Fair Credit Reporting Act:** A provision for accurate reporting and access to credit reports, requiring disclosure and reasons for adverse credit decisions
- **Equal Credit Opportunity Act:** A prohibition of any type of discrimination for credit and loan transactions
- **Home Mortgage Disclosure Act:** A requirement for lenders to collect and report data on loans they originate or purchase
- **Truth in Lending Act:** A mandate that requires disclosure of terms, fees, and annual percentage rate information for consumer mortgages, home equity loans, car loans, credit cards, and personal loans

The emergence of cryptocurrencies and digital assets in financial transactions adds another challenging dimension to fraud and financial crime prevention. Because cryptocurrencies such as bitcoin and ether use blockchain for secure processing and transaction recording, shielding the identity of buyers and sellers, money launderers, and other illegal transaction originators have an advantage when using them. Financial institutions can use partner-provided AI and machine learning solutions to detect and thwart this type of fraud.

Financial Crimes Compliance Yields Lasting Benefits

Financial institutions have much to lose when they do not sufficiently invest in fraud prevention and financial crime-fighting solutions. They risk heavy fines, sanctions, and other penalties from regulators. Failure to maintain compliance also damages their brand reputation and customer goodwill. Since the various bank failures of the 2008 financial crisis, federal and state regulators have increased scrutiny and levied financial penalties against banks that fail to adhere to statutes regarding financial crimes, especially money laundering. A strong fraud and risk management program brings lasting benefits for bank employees and customers alike. Compliance with regulations results in less operational disruption and provides account holders with an improved customer experience, fostering long-lasting relationships that drive superior financial results.

Using GenAI Technology for Regulatory Compliance

While GenAI technology is still in a nascent stage, it holds high potential in bank regulatory compliance. Many financial institutions have hundreds of thousands of past loan transactions as well as future ones that must be checked for regulatory compliance. The burden is on lenders to understand and explain "black box" credit decisions when turning down a prospective borrower. GenAI technology will be a key digital assistant for these arduous and labor-intensive compliance tasks. It will be advisory and semiautonomous, freeing human capital resources for value-added tasks. GenAI can read thousands of pages of documents quickly while identifying risks and detecting any compliance violations of past credit decisions. A GenAI system can make recommendations for corrective action on violations that can be reviewed by loan staff for changes to lending policies and procedures. In addition, GenAI will continuously monitor all state and federal lending regulations ensuring that past and pending lending decisions are in compliance while updating any new regulatory guidance or law that will impact a lender's credit decisioning process.

Considering TaskUs Compliance Solutions for Fraud and Financial Crimes

TaskUs provides outsourced financial crimes and compliance services for financial institutions. In addition, TaskUs has partnered with an ecommerce marketplace and a credit card issuing platform for anti-fraud solutions that reduce losses and preserve revenue. These services combine human expertise and AI technology to identify fraud, reduce future risks, and maintain regulatory compliance as monitored by government agencies. Humans still perform essential roles in reviewing and assessing data to make accurate decisions in situations where technology alone may have blind spots. TaskUs helps keep bank and credit union financial transactions safe against fraud and financial crime. Its digitally native customer service offerings enable omni-channel support by utilizing cost-effective non-voice channels and taking an automation-first approach to client engagements. Sophisticated security tools enable TaskUs to protect financial institutions' assets, preserve customer trust, and reduce legal and brand reputational risks.

The company's protective services for financial institutions include:

- **Identity management:** Proprietary identity solutions for KYC and KYB so that financial institutions know everything they need to know about customers, sellers, merchants, and content creators that use their platforms; safeguarding platforms that handle onboarding of accounts, online transactions, and credit card and loan decision-making
- **Compliance:** Due diligence guidance and assistance dealing with complexities of regulatory compliance for anti–money laundering, financing of terrorism, sanctions screening, and applicant risk assessment

- **Fraud:** A hybrid process drawing on human expertise and AI to thwart fraud while optimizing assets and preserving customer experience; a multilayered approach using large data sets to distinguish between legitimate and fraudulent customer transactions
- **Digital transformation:** Use of automation technology with easier deployment and better outcomes in fraud detection solutions to ensure faster quality outcomes, increased productivity, and risk mitigation

Challenges

TaskUs participates in a highly competitive market of tech vendors delivering security solutions to banks and credit unions and must continually demonstrate the differentiated essence of its services. Fraud detection and anti–financial crime measures provide financial institutions with proven value and workable solutions. However, the complex nature of financial crimes and their countermeasures requires continued monitoring and assessment. Fraudsters' methods are growing sophisticated in line with advances in compliance tools, often in a cycle of action and counteraction. Fortunately, FIs can access highly advanced AI solutions from a range of outsourcing providers that must regularly prove the uniqueness and value of their services.

Conclusion

Partnering with a financial crimes and compliance solutions provider enables financial institutions to reduce regulatory risks and avoid penalties. Providers that combine human skills and AI technology help predict and prevent future security threats. Banks and credit unions gain a competitive advantage when they work with partners that provide anti-fraud solutions. The use of cutting-edge fraud prevention and anti–financial crime measures has become especially important as the digital economy has developed into a mainstream channel for financial transactions, such as account opening, lending, and payments. In the face of fraudsters that can exploit the anonymity that digital commerce provides, an active due diligence and compliance system counteracts fraud and enables financial institutions to focus on profitability and expand their customer base.

Partnering with a financial crimes and compliance solutions provider enables financial institutions to reduce regulatory risks and avoid penalties.

About the Analyst

Raymond Pucci, *Research Director, Intelligent Finance and Customer Care Business Process Services*

Raymond Pucci is research director for IDC's Intelligent Finance and Customer Care Business Process Services (BPS) program. Raymond's research focuses on providing valuable insight into the dynamics of business process services markets. These markets include coverage of customer care, finance and accounting, procurement, and logistics business functions. This practice also provides analysis on how technology solutions and capabilities such as AI, machine learning, cloud, and analytics impact use and adoption of these business process services.

MESSAGE FROM THE SPONSOR

As someone who works closely with financial institutions every day, I've seen just how challenging it's become to keep up with the pace of financial crime. Fraud schemes are getting smarter, and staying compliant isn't just about ticking boxes — it's about truly safeguarding customers and their trust. AI, especially newer technologies like GenAI, is a game-changer. It can sift through massive amounts of data, spot patterns we might miss, and act quickly to stop threats. But let's be honest — technology can't do it all. The real magic happens when you pair these tools with skilled people who can interpret, adapt, and act. That's what we focus on at TaskUs: finding that balance between innovation and human expertise to help banks and credit unions not just meet regulations, but stay ahead in a constantly shifting landscape.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
x.com/idc
blogs.idc.com
www.idc.com