



Community Banks and Law Enforcement

A Partnership Framework
for Mutual Success

July 2026

Independent Community Bankers of America and
International Association of Financial Crimes Investigators

Table of Contents

Introduction.....	3
Building Effective Partnerships	3
Intelligence Sharing.....	3
Supporting Prosecution.....	4
Community Outreach	5
Ongoing Communication.....	5
Understanding Information Sharing.....	6
When the Community Bank is the Victim.....	6
When a Customer is a Victim	6
When the Community Bank Holds an Account of Interest	6
What Law Enforcement Needs from Community Banks	7
What Community Banks Need from Law Enforcement	7
Conclusion.....	8

Community banks can play an important role in fraud prevention as front-line observers. By leveraging their close relationships with the local customer base, community banks are often well positioned to help in the fight against fraud. With appropriate staff and training, community banks may be among the first to notice suspicious transactions, altered checks, and other signs of fraud. Early awareness can help limit further harm.

Many community banks share information with their customers about fraud risks and prevention strategies, including secure banking practices such as using strong passwords, recognizing phishing attempts, staying informed about current scams in the region, and safely handling checks. When fraud occurs, community banks may assist customers in addressing the situation and securing their accounts, and provide guidance to help them feel comfortable again.

Given the role community banks can play, they are also well positioned to cooperate with law enforcement and share information, where appropriate, to support investigations and prosecutions. This guide explains how community banks and law enforcement can build effective partnerships that benefit both parties and help hold fraudsters and scammers accountable.

This document was developed by a working group composed of community bankers from ICBA's Fraud and Scams Task Force and law enforcement professionals from IAFCI. This document is for general information purposes only and is not intended to be and should not be taken as legal advice, an endorsement of any specific company, product, or service, or a comprehensive treatment of the subject matter. Please follow internal bank operation procedures and consult with legal counsel for specific questions.

Building Effective Partnerships

In the field of investigating fraud and financial crimes, collaboration, communication, and cooperation help solve and prevent crime. Fraud prevention demands unified action with shared responsibility across the entire financial ecosystem. Success requires engaging and leveraging resources from both the public and private sectors. This means establishing true partnerships with law enforcement, other community banks, and private sector entities to ensure successful investigations and prevention.

Intelligence Sharing

Establish Intelligence-Sharing Groups: Seek opportunities to establish ongoing taskforce or multi-disciplinary team meetings with local law enforcement to maintain strong intelligence sharing. These groups help align investigations across public and private sectors, especially when targeting similar criminal activities.



Implement Secure Communication Channels: Use secure platforms for sharing sensitive information such as encrypted document exchange and cloud-based CCTV access to ensure privacy and security remain top priorities during collaborative investigations.

Utilize FinCEN's 314(b) Program: Engage in information sharing with other financial institutions and law enforcement to build a comprehensive view of criminal activity. This collaboration can uncover patterns across institutions and jurisdictions, potentially leading to breakthroughs in investigations. Recent FinCEN guidance clarifies that financial institutions may share information under Section 314(b) about activity involving suspected fraud, in addition to money laundering, terrorist financing, or other specified unlawful activities, with other eligible financial institutions.

File Detailed Suspicious Activity Reports (SARs): SARs are critical resources for law enforcement. Community banks filing SARs play an important role in helping the ecosystem prevent and detect fraud and scam activity, consistent with existing requirements.

Clarify Legal Boundaries and Processes: Law enforcement may not understand the regulations that prevent financial institutions from sharing information without due process, nor do financial institutions always understand all legal implications and restrictions placed on law enforcement. For instance, banks must follow privacy laws like the Gramm-Leach-Bliley Act, which requires banks to protect customers' personally identifiable information. Promote mutual understanding of legal and regulatory constraints to foster trust and ensure compliance during collaboration.

Share Critical Evidence: Identify and communicate what data points your community bank can retain or collect that may support investigations. Understand law enforcement's evidentiary needs to facilitate effective cooperation.

Prioritize Timely Reporting and Evidence Gathering: Speed is crucial. Most successful investigations and recoveries occur within the first 48-72 hours. Prompt reporting and evidence gathering can significantly impact case outcomes.

Align Terminology Across Sectors: Bridge communication gaps by establishing a shared language around fraud and financial crimes. This ensures clarity and reduces misunderstandings between community banks and law enforcement.

Supporting Prosecution

Provide Quality Evidence: Prosecution requires the best evidence with proper chain of custody. Thorough documentation of actions during the investigation, including videos or pictures with proper date and time stamps, will help ensure successful prosecution.

Engage with Prosecutors: Understand what prosecutors need and be available to address questions concerning reports, documents, statements, or spreadsheets. Understanding financial institution processes will help prosecutors in their efforts.



Sometimes prosecutors cannot speak with potential witnesses or victims in a case alone due to rules of justice. You can always communicate through the law enforcement investigator to establish contact with a prosecutor.

Respond Timely to Law Enforcement and Prosecutors' Requests: Prosecutors handle a multitude of criminal cases. Getting information requested in a timely fashion will not only keep the wheels of justice moving but will also help build strong working relationships with law enforcement partners. Law enforcement may need authorization for document reproduction and witness testimonies from community bank personnel.

Community Outreach

Partner to Provide Public Education: Not every crime will be prevented or solved, but through education, community banks can provide valuable information to potential victims so they are not successfully targeted. Joint outreaches can encourage victims to come forward and provide information on next steps to protect personal identifying information and savings. This can take the form of community events, nationwide efforts, or taskforce meetings.

Leverage Media as a Deterrent: Criminals watch TV and read articles. If they know your community bank has a proactive response to crime, they will normally go to a softer target. Arrests and news releases act as a deterrent. If your community bank has a reputation of seeking prosecution, criminals may think twice.

Build Customer Confidence: Customers and potential customers scour social media. By broadcasting arrests and successful prosecutions, you let your customers know that your community bank stands by them and will protect and fight for justice. Additionally, it is important for customers to understand that their personal identifying information is usually compromised through third-party businesses and institutions and not the community bank itself.

Ongoing Communication

Ongoing communication between community banks and law enforcement is essential for building trust and effectiveness. Strong coordination between banks, law enforcement, and policymakers is paramount. Partnerships can take several forms:

Joint Training Programs: Host training sessions at community bank branches to ensure both parties stay current on the latest fraud trends and detection techniques.

Working Groups: Facilitate cross-training between community banks and law enforcement to ensure a common understanding of roles and responsibilities.

Collaborative Investigations: Work together on investigations to increase timely response, pool resources and expertise, and lead to more effective identification and prosecution of fraudsters. This includes proactive outreach between community banks and law enforcement.

Understanding Information Sharing

Community banks must clearly understand and communicate the legal boundaries around sharing information with law enforcement. Before sharing information, proper legal documentation is required. If the accountholder is the perpetrator and the community bank is not subject to loss, a search warrant or subpoena is required. If the accountholder or community bank is the victim, written requests on letterhead which include a case number are needed. The specific requirements depend on three scenarios:

When the Community Bank is the Victim

If a community bank suffers a direct loss due to fraud or other criminal activity, it should cooperate fully with law enforcement. For example, if a bank incurs a \$100,000 loss and contacts their local law enforcement agency, the assigned officer should not encounter unnecessary barriers when requesting information essential to the investigation. Cooperation in these cases is not only beneficial but critical in pursuing justice and recovering losses.

When a Customer is a Victim

When a community bank learns a client has been victimized (through scams, identity theft, or unauthorized transactions), the community bank should:

- Provide guidance to the client on filing a police report and offer relevant documentation to assist law enforcement.
- If contacted by law enforcement for financial records, require the request in writing, issued from authorized agency personnel, and specific to the client's case.
- Share only the information necessary for the investigation, in compliance with privacy laws and internal policies.

When the Community Bank Holds an Account of Interest

If law enforcement identifies an account at the community bank as relevant to an investigation (such as money laundering or fraud), the community bank should continue to follow all regulatory requirements under the Gramm-Leach-Bliley Act, state statute, and internal policies and procedures.

Law enforcement must follow proper procedures when building a case, including obtaining written requests for information from authorized personnel. Confidential handling of information received from community banks is vital to build trust and encourage cooperation. While community banks may seek updates about an ongoing investigation, law enforcement is obligated to protect sources and the integrity of the case, which means they may not be able to share all information, including details received from other institutions. Understanding this limitation is key to maintaining a respectful and productive partnership.



What Law Enforcement Needs from Community Banks

Law enforcement needs evidence to identify the actors involved in criminal activity, the amount of financial loss, the specific actions used to perpetrate the crime, and, if possible, enough information to seize property for restitution or forfeiture. Community banks can provide:

Bank Records: Follow the flow of stolen proceeds through financial institutions to determine final disposition.

Video Surveillance: Positively identify actors opening accounts, conducting transactions, or making changes to accounts. Maintain CCTV footage with correct timestamps and proper chain of custody documentation.

Computer Records: Use IP addresses to determine the location of actors accessing online systems.

Withdrawal and Payment Records: Assist in identifying actors by obtaining additional records from third parties (utilities, credit card accounts, video at other locations, etc.).

Account Opening Information: Use email addresses and phone numbers provided when opening fraudulent accounts to assist in identifying actors and those with access to fraudulent accounts.

Transaction Trails: Follow stolen proceeds through multiple bank accounts to determine the identity of the actor benefiting from criminal activity and to obtain proof of money laundering activities.

Physical Documents: Obtain actual physical documents available such as identifications used, fraudulent checks provided, etc., with the intent to identify actors through fingerprinting, facial recognition software, etc.

Supporting Documents and Metadata: Sometimes, the best evidence is in the smallest details. In addition to account and transaction information, additional information may lead to the identification of criminal actors. Information such as false documents and identifications provided at the time of account opening or transaction, bad phone numbers, fraudulent email addresses, IP addresses, and even geolocation data may be available and can help the investigative process.

What Community Banks Need from Law Enforcement

For partnerships to be effective, community banks need reciprocal support from law enforcement. While law enforcement agencies face restrictions on what they can share due to ongoing investigations and legal requirements, there are critical ways they can support their community bank partners:



Case Status Updates: When permissible, provide updates on cases involving the community bank or its customers. Even general information (“the case is progressing,” “charges have been filed,” “the case has been closed”) helps community banks understand the impact of their cooperation and maintains engagement in the partnership.

Feedback on Suspicious Activity Reports: Community banks invest significant resources in filing SARs. Federal agencies like the IRS Criminal Investigation have recognized that the lack of constructive feedback on SARs has long been a major barrier to effective partnerships. When possible, share how SAR information was used, what was helpful, and what additional details would strengthen future reports. Even aggregate feedback about trends can help community banks improve their fraud detection efforts.

Clear Communication on Legal Processes: Help community banks understand what documentation is needed for successful investigations and prosecutions. Explain the difference between informal requests and formal legal process requirements. This helps community banks prepare appropriate documentation and understand their legal obligations.

Timely Responses to Bank Inquiries: Just as community banks are expected to respond promptly to law enforcement requests, law enforcement should strive to respond to community bank questions and concerns in a timely manner. This builds trust and demonstrates mutual respect.

Educational Support: Share information about emerging fraud trends, criminal tactics, and red flags that law enforcement is seeing across multiple institutions. This helps community banks strengthen their fraud detection and prevention programs.

Recognition of Partnership Value: Acknowledge the role community banks play in fraud prevention and investigation. When appropriate, recognize successful partnerships publicly, which reinforces the value of cooperation and can deter criminal activity.

Designated Points of Contact: Assign fraud liaisons who maintain regular contact with community banks. Having a consistent point of contact makes communication more efficient and helps build stronger working relationships over time.

Conclusion

Effective collaboration between community banks and law enforcement requires shared responsibility and mutual commitment. By establishing strong partnerships built on ongoing communication, mutual understanding of legal boundaries, and reciprocal support, both sectors can work together to prevent, detect, and prosecute criminal activity. Through intelligence sharing, timely reporting, public education, constructive feedback, and ongoing dialogue, community banks and law enforcement can create a united front that deters criminals, supports victims, and strengthens the financial security of the communities they serve. Success in fighting fraud demands unified action across the entire financial ecosystem, with each partner understanding and fulfilling their role in this critical mission.