Stronger Together: How Banks Collaborate on Cybersecurity

November 4, 2026

Banks collaborate with each other, with other industries and with the U.S. government to safeguard the financial system against cyberattacks. The financial sector is a leader across critical infrastructure industries in cyber information sharing, having formed the first information sharing and analysis center in 1999 and a sector coordinating council in 2002. As frontier AI accelerates and amplifies cybersecurity threats to critical infrastructure, the banking sector's proactive, collaborative coordination is more crucial than ever.

Below is an overview of the various organizations that bring together banks, other industries and/or government to coordinate defenses and responses to cyber threats.

The Trailblazer: Financial Services Information Sharing and Analysis Center (FS-ISAC)

FS-ISAC represents more than 5,000 U.S. banks, credit unions, asset managers and other financial firms. The first organization of its kind, it has shared cybersecurity intelligence for more than 25 years. Members use the forum to exchange actionable tactical and strategic intelligence with one another and the government.

The group's main U.S. government contacts are the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection.

Financial institutions actively share information on cyber adversary activities and operational disruptions with each other through the FS-ISAC's trusted communications channels as FS-ISAC monitors threats to the financial system around the globe. Information generally flows from the financial sector to the government, which uses it to inform its own activities and analysis of cyber threats. Government sharing with industry occurs through periodic bulletins and alerts on more specific threats or technical details of adversary behavior, as well as classified briefings held by Treasury's OCCIP and Office of Intelligence and Analysis and CISA-hosted briefings for critical infrastructure companies across industries.

Industry-Driven Coordination: Financial Services Sector Coordinating Council (FSSCC)

Established in 2002 shortly after the terrorist attacks of September 11, FSSCC is an industry-led nonprofit that brings together financial firms and trade associations to coordinate on critical infrastructure protection and security efforts with government agencies. Serving as a counterpart to the government's FBIIC, it helps align the industry's preparedness efforts and responses to cybersecurity threats, natural disasters and terrorism.

Its mission is to strengthen the sector's resilience against attacks by identifying threats early, promoting protective measures, collaborating with the federal government, including federal and state regulatory agencies, and coordinating crisis responses.

Government-Driven Coordination: Financial and Banking Information Infrastructure Committee (FBIIC)

Another product of post-9/11 coordination efforts, FBIIC convenes financial regulatory agencies to improve financial sector infrastructure's reliability and security. Whereas the FSSCC is driven by financial services firms, FBIIC is governed by financial regulatory agencies. The organization promotes information sharing and emergency communications protocols among financial regulators. Its three key objectives are improving coordination and communication among financial regulators; enhancing financial sector resilience; and promoting public-private partnership.

Collaborating to Reduce Risk: Analysis and Resilience Center for Systemic Risk (ARC)

The ARC is a non-profit organization founded by the largest US banks to address systemic risk within our nation's financial system. Supporting more than $7 trillion of US payments activity daily and $3 trillion in trading across equity, debt, and foreign exchange – ARC members are major providers of liquidity in the key markets that underpin our economic and national security. The organization conducts assessments of the most critical market functions and financial systems, monitors threats to those systems, and develops measures to make them more resilient.

The New Frontier: Alliance for Critical Infrastructure (ACI)

The ACI, formed in 2026, brings together multiple critical infrastructure sectors (including financial, telecom, electric, technology, transportation and water) to facilitate collaboration and information sharing on security threats. The ACI serves as a central point for critical infrastructure sectors to identify shared vulnerabilities, streamline coordination, manage crises and bolster resilience across sectors.

The group, founded by AT&T, AIG, Berkshire Hathaway, JPMorgan Chase, Southern Company and others, evolved from the Tri-Sector Executive Working Group, which was established a decade ago by banks, telecom and electric companies to strengthen coordination between interdependent critical infrastructure systems. The ACI builds on this legacy to enhance collaboration across the private sector that operates 85+ percent of critical infrastructure.

The Law Enforcement Radar: National Cyber-Forensics and Training Alliance (NCFTA)

The NCFTA combats fraud and cyber-enabled crime by bringing together financial institutions, businesses and law enforcement to share and validate intelligence, analytical and investigative resources, and fraud-prevention strategies. Through its Cyber Financial and Brand & Consumer Protection programs, it works to identify, connect, mitigate and disrupt criminal actors and networks engaged in fraud, identity theft and other cyber-enabled crime.

The group strives to provide a neutral environment for two-way collaboration and cooperation to identify and mitigate cybercrime and facilitate real-time information sharing. The organization provides a neutral forum for members across industries to share and analyze threat information, creating actionable intelligence to strengthen collective cyber-enabled crime prevention and identify civil and criminal disruption opportunities. It supports worldwide law enforcement efforts to disrupt cybercrime and has led to several successful law enforcement investigations.

More Work to Be Done

These coordination efforts are notable and provide trusted mechanisms to support the security and resilience of the financial system. As frontier AI makes it easier for bad actors to conduct attacks and execute fraud schemes, it is critical that banks be empowered to share threat data in real time with each other to safeguard the financial system.