FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, September 19, 2025

ICBA, Other Groups Call on Congress to Renew Cybersecurity Law

Source: ICBA NewsWatch Today

ICBA and other groups called on Congress to extend the Cybersecurity Information Sharing Act before its Sept. 30 expiration date, saying that failure to do so would impede public-private sector coordination during cyberattacks and weaken the nation's cyber defenses.

In a letter to Senate and House leaders, ICBA and the other groups said:

- The current cyber threat landscape highlights the need for consistent public-private collaboration, of which information sharing is a central component.
- Without the protections codified by CISA, businesses may be less willing to share cyber threat information for fear of legal exposure.

(*Click the heading link to read more.*)

Top News

Get Ready for Cybersecurity Awareness Month

Source: Cybersecurity & Infrastructure Security Agency (CISA)

October marks Cybersecurity Awareness Month, a nationwide initiative to promote safer online practices and protect individuals and organizations from cyber threats. For community banks, this is a prime opportunity to reinforce their commitment to cybersecurity not just internally, but also across their customer base.

Cyber threats continue to evolve, targeting financial institutions of all sizes. Community banks, often seen as trusted pillars of their local economies, must stay vigilant and proactive. Cybersecurity Awareness Month offers a structured approach to educating staff and customers on how to identify and respond to threats such as phishing, ransomware, and identity theft.

To make the most of October, banks should begin preparing now. A strong awareness campaign should include:

- Staff Training: Equip employees with the knowledge to identify suspicious activity, follow secure practices, and report incidents promptly.
- Customer Outreach: Share tips and resources with customers through newsletters, social media, and in-branch materials to help them protect their personal and financial information.

The Cybersecurity & Infrastructure Security Agency (CISA) provides a Cybersecurity Awareness Month Toolkit that banks can customize for their own use. This toolkit includes ready-made graphics, messaging, and educational materials designed to engage both employees and customers. It's a valuable resource to help community banks launch a professional and impactful campaign without starting from scratch.

(Click the heading link to read more.)

How to Help Protect Foster Youth From Identity Theft

Source: Federal Trade Commission

Identity theft can happen to anyone, including kids in foster care. But minors typically don't have credit reports, so they might not even realize they've experienced identity theft until they apply for a job, housing, or credit. Because foster youth often move more often and more people have access to their info, they're at greater risk of identity theft. So if you're a foster parent, a service provider, or know someone in foster care, read on for ways to help protect foster youth from identity theft.

The best place to start is with a credit freeze. Federal law says parents, legal guardians, and child welfare representatives of people under age 16 can place a free credit freeze on their behalf. The law also requires child welfare agencies to get and review credit reports every year for foster youth aged 14 and older, which can help them spot identity theft with time to address it.

- Check to see if they have a credit report. Generally, someone under 18 won't. To find out, contact the three nationwide credit bureaus and ask for a manual search for their Social Security number. Find the credit bureaus' contact information at IdentityTheft.gov. You may have to give the credit bureaus a copy of documents that prove you're the child's parent, legal guardian, or an authorized child welfare representative.
- Freeze their credit. Only an authorized adult can do this, and the process for getting a freeze for a minor is different from for an adult.

(Click the heading link to read more.)

Using FinCEN SAR Stats to Empower Community Banks

Source: Financial Crimes Enforcement Network

The Financial Crimes Enforcement Network (FinCEN) provides a powerful tool for financial institutions through its Suspicious Activity Report Statistics (SAR Stats) platform. For community banks, which often operate with limited resources compared to larger institutions, SAR Stats can be a game-changer in enhancing compliance, risk management, and strategic decision-making.

Access the SAR Stats tool here.

What Are SAR Stats?

SAR Stats are aggregated data derived from Suspicious Activity Reports (SARs) filed by financial institutions under the Bank Secrecy Act (BSA). These reports are submitted when institutions detect potentially illicit or suspicious financial behavior. FinCEN's SAR Stats tool allows users to analyze trends by:

- Industry type
- Geographic location (state, county, metro/micro areas)
- Suspicious activity categories
- Instrument and product types
- Relationships and regulators

How Community Banks Can Use SAR Stats

Community banks can leverage SAR Stats in several strategic ways:

Risk Identification and Mitigation - By analyzing SAR trends in their geographic area or industry, community banks can identify emerging threats such as:

- Check fraud
- Elder financial exploitation
- Fentanyl trafficking
- Trade-based money laundering

(Click the heading link to read more.)

Top Five Cybersecurity Threats Facing Community Banks in 2025

Source: Integris

A full 70% of banks in the US are spending more on their cybersecurity in 2025.

How do we know? We asked. As part of our latest Integris report, Understanding U.S. Banks Annual IT spend in 2025, we talked to nearly 1000 bank executives across the US, and the results were pretty consistent across the board. A full 74% of them admitted they didn't think their cybersecurity spending was effective in 2024–and they want to do something about it.

With the cost of data breaches continuing to rise, it's not hard to see why. According to IBM's 2024 Cost of Data Breach Report, financial services have more to lose than nearly any other business sector, with losses topping $6.08 million per breach last year, compared to the national average cost of $4.88 million.

As hackers continue to up the ante with ever more sophisticated attacks, it's tempting to dump big chunks of your IT budget on the latest shiny new cybersecurity tools. That's great, but in my experience, the road to cyber safety has never been paved with quick fixes. If you truly want your bank to have future-focused, compliant cybersecurity, you'll need to think holistically about your entire information technology portfolio, your IT infrastructure, and the way your staff and customers interact with it.

To demonstrate what that looks like for the average bank, I'm going to discuss what I think are the five biggest cybersecurity threats banks are facing in 2025, and how to meet them head on.

Threat #1—A Lack of a Written AI Fair Use Policy
Many banks are taking a "wait and see" approach to implementing new artificial intelligence tools at their bank, and that's fair enough. Yet, that doesn't mean that AI isn't being used in your bank every single day.

(Click the heading link to read more.)