FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, April 3, 2026

Synthetic Identity Fraud: A Guide for Community Banks

Source: ICBA

Synthetic identity fraud is one of the most difficult fraud types for community banks to detect, and by several industry measures, it's also one of the fastest growing. In the February issue, I examined how criminals are using artificial intelligence to accelerate fraud. Synthetic identity fraud is a natural extension of that threat.

Synthetic identity fraud occurs when a criminal combines real, personally identifiable information like a Social Security number with fabricated details like a fictitious name or date of birth. The resulting identity does not belong to any actual person, yet it can pass standard verification checks. The Federal Reserve has published extensive research on this problem and reports that synthetic identity fraud is responsible for billions of dollars in annual losses.

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

Top News

Behind the Scam: How Fraudsters Use Social Media, Software, and Shell Companies to Steal Millions

Source: Organized Crime and Corruption Reporting Project

At the heart of many modern-day scams is the call center: sleek offices staffed by manipulative, multilingual agents who spend their days trying to convince victims from around the world to pour funds into fake investment opportunities.

These call centers, however, do not operate in a vacuum. They draw upon an entire ecosystem of service providers who help facilitate each step of the process — and get a cut of the profits.

Here, we present dozens of companies from around the world whose services were used by the two large-scale fraud operations exposed by Scam Empire, one based in Israel and Europe and the other in the country of Georgia.

It was not always possible to determine the extent to which these companies were aware of the scams their services helped facilitate.

From external marketers who harvest victims' data to money transfer services used to extract their cash, these players range from legitimate businesses exploited by the scammers to entities that appear purpose-built to help them carry out their nefarious work.

Below we have organized these providers by their role in the three major phases of a scam: catching victims, winning their trust, and taking the money.

(Click the heading link to read more.)

Fraud Awareness and Prevention Social Media Communications

Source: Cross Financial

Fraud prevention has become a critical priority for community banks, and social media offers a powerful way to connect with customers through timely, consistent education. A successful fraud prevention social media campaign combines clear messaging, practical tips, and visual reinforcement, an approach outlined in Cross Financial's Fraud Prevention Communication Ideas 2026.

The Cross Financial framework provides a structured 12-week social media campaign designed specifically for community banks. Each weekly post focuses on a core aspect of fraud awareness, including recognition of common scams, understanding fraudster tactics, and knowing how to respond when suspicious activity occurs. Posts follow a simple, repeatable format: headline, short explanation, single actionable tip, and suggested visuals, making the content easy for customers to understand and easy for banks to deploy.

Key campaign topics include phishing and smishing scams, fake urgency messages, caller ID spoofing, protection of personal information, and steps to take if fraud is suspected. By addressing these risks individually over time, the campaign reinforces learning and avoids overwhelming customers with too much information at once. Consistent themes such as "pause and verify," "never share passwords or verification codes," and "contact your bank directly" help consumers build safer habits.

(Click the heading link to read more.)

Yes, Your Personal Information Is For Sale. Here's What to Do About It

Source: IDX

If you've ever Googled your own name, you've likely seen search results from sites with names like Intelius, MyLife, PeopleFinder, or Spokeo. They seem to know a surprising amount about you—not only your age, address, and phone number, but things like your homeownership status, your tax records, your court records, your voting records, or your religious affiliation.

You've probably had questions about these sites. What are they, exactly? How do they know so much about me? It seems like an invasion of privacy and an invitation for identity thieves—is this legal? Here are some answers.

Data Brokers: Legally Gathering and Selling Your Information

The sites promoting your personal information are called data brokers, a.k.a. "people search" sites. There are more than 100 of them currently operating; they scour the internet collecting people's data, then sell it to advertisers and other groups. And it's completely legal for them to do so.

These sites use automated software to harvest your information from tech companies, telecommunication providers, credit bureaus, tax records, court records, DMVs in some states, and other public sources. They bundle your data into a comprehensive personal profile, which they can sell to any person or group willing to pay a few dollars. (A typical report costs $20.)

There are three main privacy and identity risks involved when data broker sites sell your personal information:

(Click the heading link to read more.)

Leverage Branches as Effective Learning Hubs in the Fraud Fight

Source: ProSight

Branch leadership can think creatively even when it comes to one of the most serious issues facing banking today: minimizing fraud.

ProSight regularly engages with fraud and cybersecurity experts who stress that as routine banking reaches across several channels, branches provide a personalized and conversational atmosphere, focused audience attention, including personnel, plus traction within the community. Targeted fraud education efforts might include well-placed signage, inviting small business leaders for in-person workshops on detecting fakes from a batch of legitimate checks, or hosting breakroom pub-style quizzes and mocktails to test staff knowledge of phishing.

"Given the seriousness of risks and the range of fraud vectors, anti-fraud messaging in statement inserts and emails that may get lost in a mix of all-bank messaging just doesn't cut it anymore," said Bobbie Paul, managing director, fraud, at consultancy Huron, who led a ProSight Banking Trends webinar on prioritizing fraud prevention goals in 2026.

Because fraudsters are regularly upgrading technology and expanding their reach, including with AI, strategists advise addressing fraud-protection steps early and often in banking relationships.

(Click the heading link to read more.)