FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, June 12, 2026

Cyber Risk Is Business Risk, Making Captives Even More Valuable

Source: Hylant

Sit down with a group of risk management professionals these days, and one topic will definitely come up at least once: cyber. Regardless of the subject of the discussion, cyber will inevitably pop up like a whack-a-mole game.

That's because cyber never sits still. The threat environment keeps evolving, and risk managers race to shift coverage where it's needed most. Last year's solutions may not be enough for today's threats. For technology-dependent organizations, the stakes keep getting higher.

Why Business Risk and Cyber Risk Are Now Intertwined

There's a simple way to understand why cyber is so pervasive: IT risk is business risk, and business risk is IT risk. That may seem obvious, but it represents a fundamental shift in risk management philosophy. For years, companies have treated cyber as though it were solely a technical issue, pushing it off on those people in IT. Today, company leaders recognize that cyber is an operational issue, a financial issue, and can easily become a reputational issue affecting a company's long-term viability.

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

Top News

2026 Fraud Insights - U.S. Payments Edition

Source: NICE Actimize

The fraud landscape is advancing at a sustained and measurable pace, with both attack frequency and operational complexity increasing over the past year. Emerging fraud typologies, increasingly sophisticated social engineering techniques and the rapid maturation of fraudster-led AI have collectively expanded the scale, speed and crossborder impact of global fraud activity.

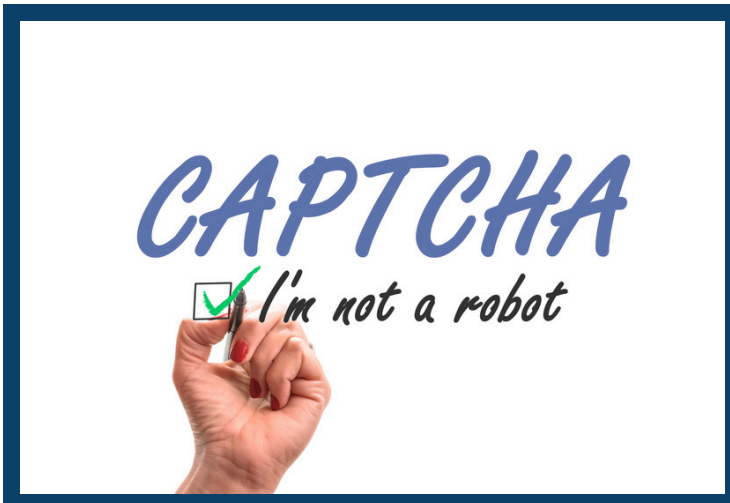
These shifts have not only captured public attention but have also intensified regulatory pressure on financial institutions (FIs), raising expectations for stronger, more adaptive fraud mitigation frameworks.

In the 2026 edition of the NICE Actimize Fraud Insights Report, we extend our analysis across the U.S. payments ecosystem to deliver a consolidated, data-driven view of today's fraud environment. By examining trends in both genuine and fraudulent transactions, we highlight where structural shifts are occurring, identify emerging patterns across payment types and pinpoint where fraud pressure is intensifying.

This report provides actionable intelligence to help institutions anticipate and respond to an increasingly dynamic threat landscape.

The findings in this report highlight an increasingly important theme in modern fraud prevention: the need for stronger industry collaboration to address networked and coordinated threats. This shift is not theoretical — it is already reshaping how institutions approach detection and treatment.

(Click the heading link to read more.)



How To Spot a CAPTCHA Scam

Source: Federal Trade Commission Consumer Advice

The FTC is getting reports about a new phishing scam that looks a lot like the CAPTCHA requests you might be used to seeing. Real CAPTCHAs give you image- or text-based tasks to prove you're not a robot — something like typing letters and numbers exactly as they appear, or matching pictures of things like fire hydrants or traffic lights. Here's how the fake CAPTCHA requests happen...and how you could wind up installing malware on your own device.

You get an unexpected CAPTCHA request while browsing a website. The screen looks a lot like a regular CAPTCHA, asking you to verify you're human. But the message says to type a series of commands — something like "Windows + R," then "Ctrl + V," and then "Enter". The screen might say "security verification," but you're actually following the steps to paste and run hidden malware on your device. Once it's there, scammers can quickly steal your email account login data, mobile banking credentials, or any other information they can get access to.

Real CAPTCHAs won't ask you to run commands on your device. If you notice something downloading to your device after responding to a CAPTCHA, act quickly to remove the malware and protect yourself:

- **Disconnect from the internet**. This stops scammers from accessing your online shopping or banking accounts.
- **Run a security scan to remove the malware.** Keep your software and apps up to date to catch viruses.

(Click the heading link to read more.)

X9 Releases Report on Mitigating Check Fraud

Source: Accredited Standards Committee X9

The Accredited Standards Committee X9 Inc. (X9), the organization accredited by ANSI to develop financial industry standards for the United States, announced the publication of an informative report, "Mitigating Check Fraud Risk in the Modern Financial Ecosystem." X9 is also launching a broad, open industry forum that will cover all types of payment fraud, incorporating the existing check fraud forum under its umbrella.

The new report provides the financial industry with actionable strategies to mitigate fraud risk while balancing operational efficiency and customer trust. It includes an assessment of the current check payments landscape and examines the financial impact of check fraud on the industry. Key findings from this report will be incorporated into X9's Technical Report 8: Check Security. The new document is now available for download without charge.

Specifically, the informative report:

- Outlines check fraud categories and scenarios
- Evaluates detection and prevention tools and strategies
- Offers procedural recommendations alongside high-level regulatory reminders
- Provides details related to educational plans for financial institution employees and customers

Background

Despite the rapid adoption of digital payment systems, nearly all businesses still use checks for some financial transactions. Consumers continue to use checks for various expenses, and government entities also issue many benefits via check. Checks thus remain a viable and increasingly targeted instrument for fraud. Criminals have now adapted traditional fraud techniques to exploit various points in the check payment ecosystem.

(Click the heading link to read more.)

Medicare Fraud Affects Everyone, So Here's What To Know and Do

Source: Federal Trade Commission Consumer Advice

Medicare losses due to fraud, errors, and abuse cost taxpayers about $60 billion every year. Providers might double-bill Medicare for a single treatment, charge for things like a back brace you didn't get (or need); a company might offer you a fake Medicare drug plan; or a scammer might ask you to confirm your Medicare number — which they then use to commit hospice fraud.

Medicare fraud, abuse, and unintentional errors can also contribute to medical identity theft, losing your benefits, and paying higher medical costs. So, what can you do to help fight Medicare fraud while protecting yourself and your community?

- Never share your Medicare number with someone who calls unexpectedly. **Medicare won't call** or visit you at home to sell you anything. Medicare representatives will only ask for information if you contact them first.
- Review and report Medicare fraud and abuse. Spot mistakes or inconsistencies in your statements? Ask your medical provider or plan to explain. If you suspect fraud or abuse, call 1-877-808-2468 to reach your local Senior Medicare Patrol, or call Medicare at 1-800-MEDICARE.
- Report medical identity theft. If someone uses your information to get medical care or services, notify your provider or plan. And report the theft to IdentityTheft.gov to get a personalized plan to help you recover.
- Learn more about protecting and recovering from medical identity theft. Join the FTC, the...

(Click the heading link to read more.)