FRAUD PREVENTION FRIDAY

Community Bankers of Michigan

Friday, November 13, 2026



Using 'Appropriate Friction' to Stop Scams in Digital Banking

Source: ICBA Independent Banker

For years, good digital banking meant removing friction: fewer clicks, faster logins and instant transfers. Scammers have proven adept at taking advantage. They create urgency, keep the victim on the phone and move the money before anyone can intervene.

That speed is one of the challenges community banks face. As I wrote in September, most successful investigations and recoveries take shape within the first 48 to 72 hours, and the FBI's Recovery Asset Team depends on banks acting quickly to freeze funds before they disappear. Community banks can use appropriate friction to extend the time available to detect and mitigate scams.

Appropriate friction is targeted. The goal is not to slow every payment. The pause is for the transactions that look like scams: a first payment to a new payee, an unusual amount or a new device paired with an urgent transfer. Many customers will accept a small delay when it improves...

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

Top News

- Using 'Appropriate Friction' to Stop Scams in Digital Banking
- When the Legitimate Tool is the Intrusion
- New Report on the FTC's Work to Protect Older Adults
- Internal Controls Prevent Fraud
- Cyber Incident Reporting Form: Frequently Asked Questions



When the Legitimate Tool is the Intrusion

Source: Q6 Cyber

How criminals use RMM software to bypass the controls designed to stop them.

A remote support session opens on a computer. The software is a commercial remote monitoring and management (RMM) platform. Its publisher is trusted, its installer is digitally signed, and it's probably not on your organization's block list.

The person on the other end might be your help desk or it might be someone who was recruited, trained, and paid to sound like your help desk: "Mark from IT," a fraudster who doesn't work for your company and who may not even be a human.

But this session could also be running on your customer's personal device. The caller says they're from your fraud department and they walk your customer through installing that same tool.

To the controls in place to catch fraud, these sessions look identical. Both use the same tool, the same signature, and the same traffic to the same legitimate domains. Spotting these sessions is the kind of work Q6 does for banks and credit unions every day: collecting information from the Dark Web and private criminal channels and delivering our analysts' findings to our clients' fraud teams so they can act on it before fraud can occur.

What RMM tools are

RMM platforms are built for IT administration. Internal IT teams use them to manage corporate endpoints, help desks use them for remote support sessions, and organizations with hybrid workforces or several locations rely on them to manage devices from a distance. They're designed to provide persistent, interactive access to a system, and to keep running quietly in the background.

(Click the heading link to read more.)



New Report on the FTC's Work to Protect Older Adults

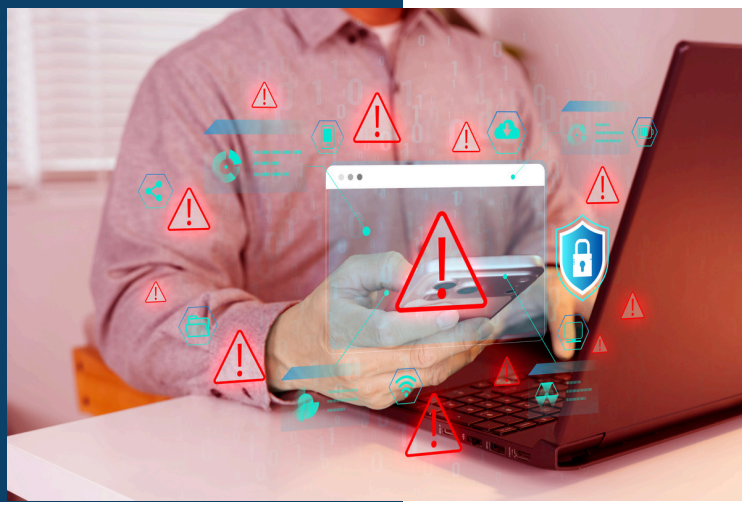
Source: Federal Trade Commission Consumer Advice

Protecting older adults is a top priority for the FTC, and a new report to Congress outlines how the agency has taken this on. From law enforcement to consumer education to coordination with partners, the FTC's taken a multi-faceted approach to combatting fraud and other issues affecting older adults over the past year. Check out the report for updates on new scam trends, FTC cases that impacted older adults, and consumer education resources like Pass It On.

What are some highlights?

- **Research and data analysis**: From 2020 to 2025, total fraud losses reported by older adults (ages 60 and over) increased from $600 million to about $3 billion. And last year, while younger adults were generally more likely to report losing money to fraud than older adults, older adults were more likely to report losing money on certain types of scams including tech support, prize, and government impersonation scams.
- **Enforcement actions**: Recent FTC law enforcement actions that impacted older adults focused on various consumer protection areas including debt relief services, health insurance frauds, government and business impersonation schemes, money-making opportunities, and tech support scams.
- **Outreach to older adults**: Recent collaborative efforts included initiatives like Never Ever, a public-private consumer education campaign that raised awareness about government and business imposter scams. (You can find and share the campaign's materials here.)

(Click the heading link to read more.)



Internal Controls Prevent Fraud

Source: Rehmann

Fraud costs organizations more than $7 billion annually, according to the Association of Certified Fraud Examiners' (ACFE) latest "Global Report to Nations."

And those are just the hard costs. They don't account for reputation loss and poor public opinion, which can be impossible to overcome.

Nearly half the cases in the ACFE study were due to weak internal controls. While there's no guaranteed way to stop fraud, improving internal controls can strengthen every organization.

Culture is Critical

If the "tone from the top" indicates buy-in and high prioritization of strong internal controls, it permeates the entire organization.

But it can't be only talk.

Policies must be enacted, followed and enforced proactively. Asking questions is good. The best internal control environments focus on collaborative and continuous improvement.

Opportunities to better safeguard assets and information occur frequently, whether it's an everyday process or annual audit. When people are empowered to challenge and ask questions, positive changes can take hold. Invest in and reward that behavior.

Systems, Policies and (Most Importantly) People

Internal controls must address every aspect of an organization, especially information technology (IT) because we rely on it so much.

Systems must be designed with checks and balances in place, especially financial systems. That includes IT systems and work processes like expense reviews. Along the same lines, IT policies which are established by...

(Click the heading link to read more.)



Cyber Incident Reporting Form: Frequently Asked Questions

Source: Cybersecurity & Infrastructure Seurity Agency

What is the cyber incident reporting form?

The cyber incident reporting form, updated in 2026, is an enhanced questionnaire used to submit incident information through CISA's Incident Reporting Portal. The form incorporates widely accepted government and industry frameworks, standards, and principles. CISA developed the form using feedback from incident response partners and subject matter experts.

Why did CISA change the cyber incident reporting form?

The new form enables reporters to provide critical information CISA needs to better support cyber defense and incident response for both the reporting organization and broader cybersecurity community. The new form captures normalized data and information that is detailed and actionable information that helps CISA quickly assess incidents and prioritize response actions. The improved cyber incident reporting strengthens CISA's ability to understand the threat landscape and respond to cyber risk.

What has changed in the cyber incident reporting form?

The updates to the form include removing duplicative questions, improving accuracy across reported incidents, and enabling better triage and enterprise response. This update improves the utility of incident reporting information and the user experience for all CISA stakeholders.

(Click the heading link to read more.)