FRAUD PREVENTION FRIDAY

Friday, September 20, 2024

Introducing a Customizable Anti-Fraud Tool for Bankers: Protect Your Customers from Scams

Fraud and scams continue to rise in the financial world, targeting consumers of all ages and financial backgrounds. As technology becomes more advanced, so do fraudsters' tactics. Bankers are on the front line, working to protect their customers' financial well-being. However, the challenge has always been finding an effective, customer-friendly way to educate and protect individuals from these threats.

Now, with the increasing demand for proactive fraud prevention, we, in partnership with CBM Preferred Partner SHAZAM, introduce a customizable anti-fraud tool that banks can brand with their own logo. This tool empowers bankers to build stronger, trust-based relationships with their clients.

The tool linked in the title above contains questions front-line staff should become comfortable asking their customers before they become victims. By educating customers about fraud and scams, banks can significantly reduce the financial losses associated with fraud.

(Click the link above to access the Fraud Prevention Questions)

Top News

P2P Payment Fraud Is on the Rise: How To Combat It

The launch of PayPal in 1998, along with the growing adoption of mobile technology, ushered in what has become one of the most popular forms of payment today: peer-to-peer, or P2P, payments. As with each new type of payment option, P2P payments offer both benefits and risks to consumers and community financial institutions (CFIs).

Roughly two-thirds of smartphone users in the US (or about 170MM people) will send a P2P payment in 2024, and this is projected to increase to three-quarters of smartphone users (or nearly 200MM people) by 2028, according to a forecast by eMarketer. Total P2P transaction volume in the US is projected to increase from $1.4T in 2023 to $2.3T by 2026.

Ripe Targets for Fraud
The main aspects of P2P payments that make them so popular — convenience, speed, and accessibility — also make them ripe targets for fraud. Consumers love the fact that they can transfer money to friends instantly with just a few clicks. Unfortunately, so do thieves and fraudsters, who find it relatively easy to assume others' identities and steal these fund transfers.

Around 8% of banking customers reported being the victim of a P2P payments scam in a 2023 report by J.D. Power. While still a low proportion, this number will likely increase as P2P payments become more common and scammers become more versed in their tactics on these platforms. More concerning are the losses consumers have reported. The Federal Trade Commission reported receiving around 65K consumer complaints about P2P fraud payments, with consumers suffering $210MM in losses in 2023. These losses have been climbing steadily each year, with 2021 data reporting $130MM in losses and 2022 losses totaling $163MM.

(Click on the link in the title to continue reading.)

Don't Take The Bait on Phishing Scams

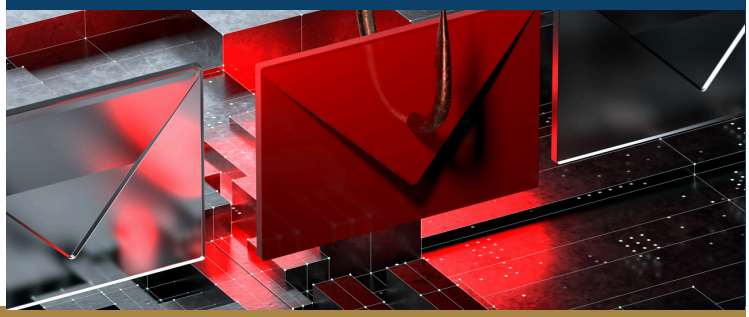
The Federal Trade Commission published the following article. Community bankers are encouraged to share this information with their customers to help keep them safe from falling for these scams.

Have you ever gotten a text or email warning you that something is wrong with an account online? Maybe it says your streaming account is about to be suspended unless you respond quickly. It might even have a link that will supposedly fix your account's problems. The message looks real. But is it?

Your first instinct might be to click to solve your problems. Don't click. There's likely nothing wrong. Instead, it might be a phishing scam. That's when scammers pose as well-known companies to get you to give up sensitive information via text or email. A phishing email might:

- say they've noticed some suspicious activity or log-in attempts — they haven't
- claim there's a problem with your account or your payment information — there isn't
- say you need to confirm some personal or financial information — you don't

(Click on the link in the title to continue reading.)



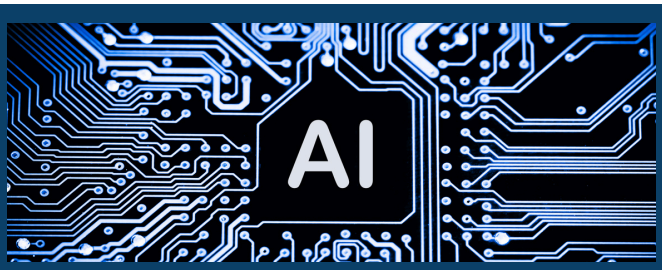
The Critical Role of Customer Fraud Education in Community Banking

Community banks have a responsibility to protect their customers from fraud. It's important for them to educate customers about the latest scams, such as phishing, identity theft, and social engineering. By doing so, banks not only prevent financial losses but also build trust and loyalty with their customers. This proactive approach can reduce fraud-related disputes and safeguard the bank's reputation. Well-informed customers are more likely to recognize threats, report suspicious activity, and take necessary actions to secure their accounts, benefiting both themselves and the bank.

Here are some effective approaches:

- Host in-person or virtual workshops where bank representatives explain common fraud scams (like phishing, identity theft, and phone scams) and how to avoid them. These can be conducted at the bank or in partnership with local community centers.
- Distribute brochures, posters, and infographics highlighting different types of fraud and how customers can protect themselves. Place these materials in high-traffic areas of the bank and on the bank's website.
- Regularly send out educational content via email or SMS, explaining the latest scams targeting banking customers and providing tips on how to stay safe.
- Offer online resources, such as webinars and video tutorials, that provide in-depth guidance on recognizing and avoiding fraud. These can be promoted through the bank's website and social media.
- Dedicate a specific month to fraud awareness, during which special events, promotions, and information sessions are held to educate customers on the risks of fraud.
- Use social media platforms to share quick tips, alerts on recent scams, and engaging content, such as quizzes or short videos that educate customers on fraud.
- Ensure customer service representatives are well-trained on fraud issues to assist customers effectively when they report suspicious activities or ask questions about scams.
- Integrate fraud awareness tips directly into the bank's mobile app. These could be in the form of pop-ups or notifications warning about recent scams or providing advice on account safety.
- Collaborate with local law enforcement to provide expert advice during events or through shared educational campaigns, adding credibility to the bank's fraud prevention efforts.

By implementing a mix of these strategies, community banks can effectively educate their customers and help them stay vigilant against fraud.



AI Agents, Can They Fight Fraud?

Register for this free webinar to learn how AI Agents can help fight fraud. Andrew Stone from CBM Preferred Partner BHG Financial is one of the speakers. The webinar will take place on Thursday, October 3, at 12:00 PM EST.

For the low price of $200/month, opportunistic fraudsters and organized crime rings can now pay for a subscription for FraudGPT. And they are — often using the "dark LLM" to draft bank-related phishing emails (and even suggested where in the content people should insert a malicious link), generate highly convincing fake financial documents, create realistic synthetic identities, and craft persuasive narratives used in social engineering scams.

But there is hope for fraud fighters in a groundbreaking technology powered by LLMS: AI Agents. In fact, 83% of executives at companies with more than $1B in revenue plan to integrate AI Agents within the next three years. So what are AI Agents? And how will they empower — and not replace — frontline fraud fighters? Tune into this live recording of the Good Question podcast to find out.

Here's what you'll learn:

- Learn how criminals use FraudGPT to create advanced phishing emails, fake documents, and social engineering scams.
- Discover why 83% of executives at large companies plan to integrate AI Agents for fraud prevention within the next three years.
- See how AI agents won't replace frontline fraud fighters; each fraud fighter will evolve into a manager of AI risk agents.

(Click the link in the title to register.)