



AI Is Fueling Fraud.

Here's How Banks and Businesses Can Prevent It.

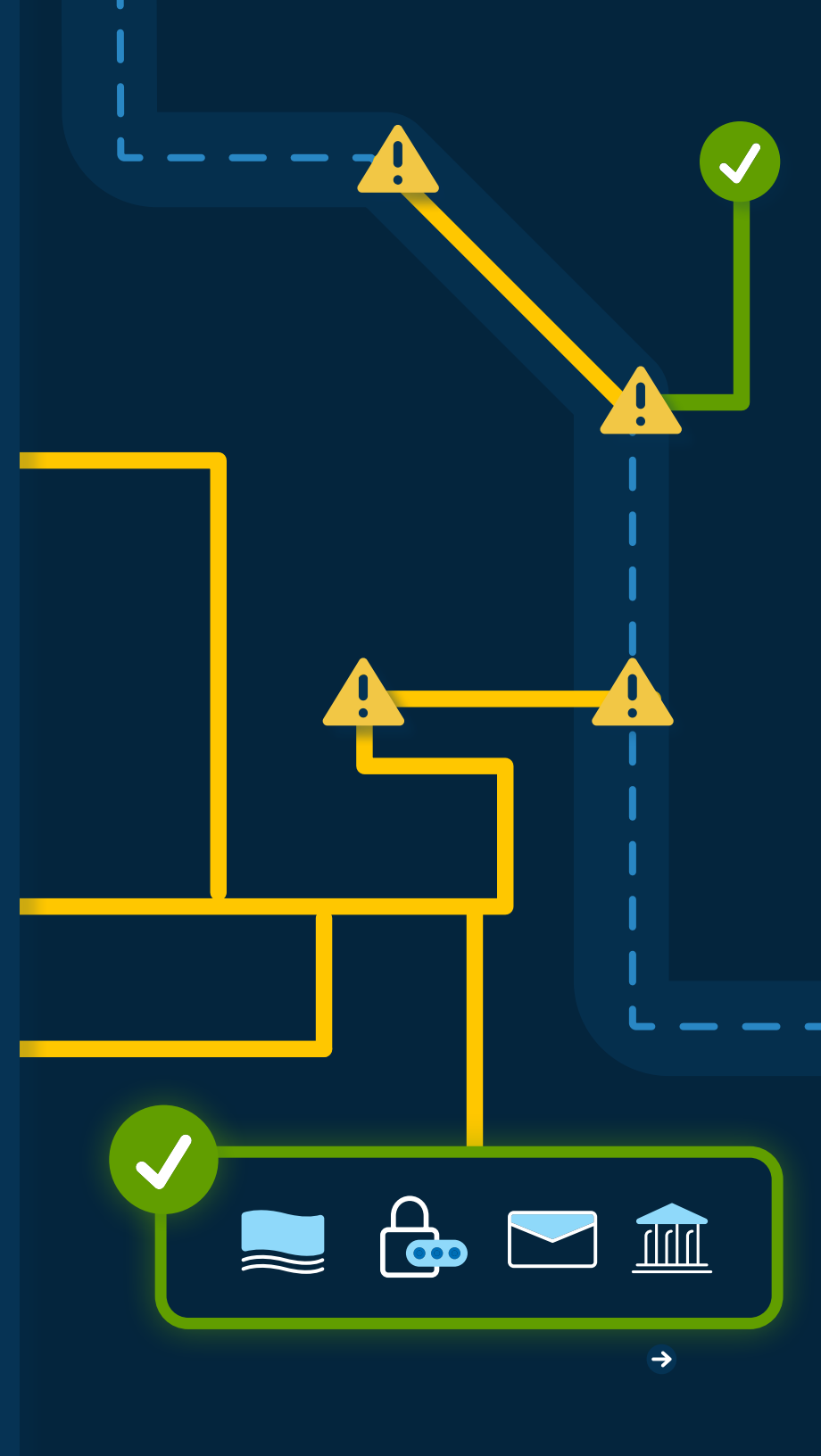
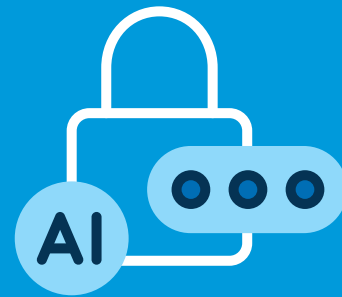


Table of Contents

- 5** Executive Summary
- 7** How AI is Making Fraud Easier for Bad Actors
- 11** AI is Creating New Frontiers in Fraud
- 14** How AI Is Making Existing Fraud Schemes Harder to Detect
- 18** Fighting Back Against AI Fraud with a Layered Approach
- 24** What Businesses Must Know about AI Fraud
- 25** Test Your AI Fraud Knowledge
- 26** Fraud Prevention Methods to Remember



Financial fraud is advancing rapidly, and with each shift, detection and prevention become more challenging. AI is not only increasing the urgency of existing fraud but creating a new set of fraud risks that didn't exist before.



In 2025, over half of all fraud attempts involved AI platforms like ChatGPT and Claude, according to AI fraud prevention firm Feedzai.¹ The problem is only expected to get worse, with Deloitte estimating \$40 billion in US fraud losses from AI-related crimes in 2027.¹

AI makes fraud schemes and scams easier to scale, harder to detect, and potentially more lucrative than ever. Businesses and banks must protect themselves, but challenges abound. Banks must navigate complex regulatory environments, businesses face budgetary crunches and technology gaps, and bad actors have a head start in both adoption and freedom to use AI tools effectively.



The threats are growing.
So must our defenses.

—**Dalit Amitai**, Head of Product and Technology for Fraud Solutions, Bottomline

Executive Summary

For banks and businesses to win even when the odds are stacked against them, they must fully understand the threat and proactively develop effective prevention and detection strategies.

STATISTICS

- + **Over half of all fraud attempts** involved artificial intelligence²
- + **49% of businesses and banks** do not use fraud monitoring technology, AI or otherwise³
- + **\$40 billion in AI-related fraud** losses are expected by 2027¹

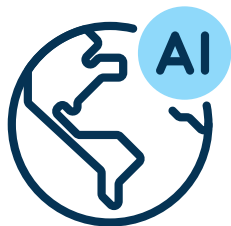
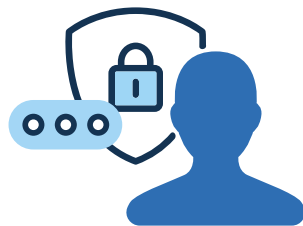
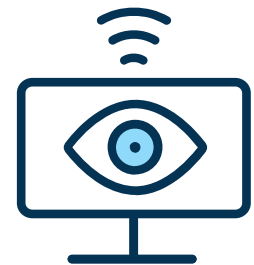
TAKEAWAYS

- 🔍 Deepfakes, AI-created invoices, and IT impersonation are **newer AI-aided schemes**
- 🔍 Account takeovers, Business Email Compromise (BEC), and insider fraud are **turbocharged by AI**
- 🔍 Using AI effectively, partnering with fraud practitioners, and training employees is key to **preventing losses from AI-enabled fraud**



In this guide, we'll share fraud trends, practical advice for combatting AI-based schemes, and share specific insights from Bottomline experts **Albert Laino**, Senior Solutions Consultant for Digital Banking, and **Katie Elliott**, Senior Risk and Fraud Officer for Paymode.

They discuss the scope of AI fraud and how it's creating new threats and augmenting familiar ones. Plus, they'll give practical steps organizations can take to shield themselves from losses and reputational damage.





How AI is Making Fraud Easier for Bad Actors

Typo-riddled emails, blatantly fake invoices, and brute force attempts to crack passwords are only so effective, needing a wide-ranging effort to steal credentials, compromise accounts, and funnel funds elsewhere.

Even though it didn't take much effort to send an email blast, only a small percentage of targets fell for it if the attempt lacked credibility. That meant that despite the scale of fraud, businesses and banks with well-trained employees and strong systems kept a certain level of safety.

Fraudsters have typically been constrained by two challenges: capability and scale. That has changed.



FRAUD UPTICK BY THE NUMBERS

In 2025,

99% of email addresses had been targeted by fraudsters⁴

79% of businesses saw an increase in fraud last year⁵

80% of businesses reported experiencing a fraud attempt⁵



While the prevalence of these attempts grows, so too does the sophistication of schemes like **account takeovers, BEC, and phishing.**

4. ProofPoint 5. AFP





THE FRAUD EXPERTS
POINT OF VIEW

Albert Laino

AI is helping fraudsters exploit gaps, and these gaps are not just looking at different policies or different systems, but also their flaws and weaknesses.

We're talking about gaps in how we can infiltrate trust and human behavior. What we're seeing with fraudsters using AI is that they're trying to really enhance and scale their social engineering, how they're automating the process of gathering information on their targets and executing these campaigns.





THE FRAUD EXPERTS POINT OF VIEW



Katie Elliott

AI is much more prevalent, and it is helping us from a fraud prevention standpoint as well as helping fraudsters perpetuate swindles. I think the fraudsters always tend to be a little bit ahead of us in terms of adopting new tools. Businesses have to vet those tools first, which is why it almost feels like we're chasing them versus a proactive approach.

We would all love to be ahead, but somehow, they get their hands on the tools and find a way to use them for evil faster than we can use them for good to catch them.



AI is Creating New Frontiers in Fraud

While deepfakes, IT impersonation, and vishing (voice phishing) are not strictly new, they are rapidly emerging as some of the most advanced and dangerous schemes out there.

AI's ability to convincingly mimic faces, voices, messages, and even whole identities have made it so that swindles that made you roll your eyes in the past are now far more believable and harder to detect.





DEEPPFAKES & VISHING

While technical glitches and awkward phrasing can still provide clues, **deepfakes via video and calls are getting extremely convincing.**



IT IMPERSONATION & CREDENTIAL THEFT

A twist on traditional phishing schemes, this one relies on the novelty of being directly messaged through your workplace communication tools **by someone who appears to be from your IT team.**



AI-CREATED INVOICES

Fraudsters can spend as little as \$10 on black market services or exploit AI to generate invoices that are extremely difficult to distinguish from the genuine article.

WHAT IT LOOKS LIKE IN PRACTICE:



Your CEO calls you directly telling you an invoice must be paid urgently and to pay it into a new account.

The message sounds and looks just like him.

By the time you realize it's a deepfake, the money has been transferred and is gone.



A member of your IT team messages you on Microsoft Teams and says there has been a data breach and you need to log in via a new secure portal; despite the contact information checking out, this is a fraudster looking to swipe your credentials and hack into your systems.



You're expecting an invoice to arrive from Martin's Printing Co., and one shows up. The amount seems correct and so you pay it with a check without double checking, and there goes your money.





THE FRAUD EXPERTS POINT OF VIEW



Albert
Laino

AI is much more prevalent, and is helping us from a fraud prevention standpoint as well as helping fraudsters perpetuate scams.

Scammers can potentially do things such as mimic speaking to your CFO and having their exact mannerisms and voice inflections incorporated into a deepfake.

It's making it difficult to assess the payment authorization process. High personalization in these scams is making it more difficult for us as fraud practitioners to find and uncover these potential risks until it's too late.



Katie
Elliott

Scammers can potentially do things such as mimic speaking to your CFO and having their exact mannerisms and voice inflections incorporated into a deepfake.

It's making it difficult to assess the payment authorization process. This high personalization in these scams is making it more difficult for us as fraud practitioners to find and uncover these potential risks until it's too late.





How AI Is Making Existing Fraud Schemes Harder to Detect

“It’s the same kind of fraud, just on AI steroids.”

That’s how Bottomline Senior Risk and Fraud Officer Katie Elliott describes traditional schemes like account takeovers, BEC, and insider fraud in 2026 and beyond. These supercharged schemes use AI to make traditional schemes more difficult to uncover and easier for fraudsters to deploy across a broader range of victims.





ACCOUNT TAKEOVERS

A bad actor can prompt AI to generate a convincing bank login page. While the AI tool may object, savvy fraudsters can get around safeguards. The fraudulent login page is then launched online; search results get manipulated to have it show up near the legitimate sites, and phishing emails are sent with the fraudulent login page linked. If the page is convincing enough, fraudsters can get a handful of users to input their legitimate login credentials—and then their account ends up in the wrong hands.⁶



**77% of finance leaders
consider account takeover
a top fraud concern.⁶**





BEC & PHISHING

The typo-ridden emails of the past are fading as fraudsters use AI to craft more polished, convincing messages to request credentials, redirect payments, or import malware.

AI also helps them find the right targets— both businesses and users— more effectively, given that there's so much data available for AI to refine targeting. And with tools like ChatGPT and Claude now widely used for legitimate purposes, knowing that an email is "AI-generated" is no longer such a clear warning sign. Once inside the victim's inbox, these messages can lead to impersonation, data exposure, and fraudulent payments.

Businesses
suffered \$2.8 billion
in business email
compromise losses in 2024.⁷

7. NACHA



INSIDER FRAUD

Katie Elliott notes that where there's opportunity, there's the risk of insider fraud, and opportunity is growing thanks to AI.

With sensitive information accidentally exposed to internal AI instances and the technology's willingness to offer workarounds and plausible excuses for accessing sensitive systems, bad actors on the inside of companies find fraud easier to execute. The ability to deepfake approvers all combine to make this kind of insidious fraud both harder to detect and potentially more lucrative for a corrupt employee.

93% of
business leaders
say insider fraud is harder to
detect than external threats.⁸

8. SentinelOne





THE FRAUD EXPERTS POINT OF VIEW



Albert
Laino

In terms of social engineering, AI is really focused on removing friction for the fraudster or the attacker. With schemes such as credential theft, AI is making it easier to procure diverse types of username and password types of lists, making phishing more convincing and hyper-targeted. Mimicking the internal user or the employee usage of an application is also a favored tactic.

This is blending and skewing the lines between normal activity and nefarious activity.

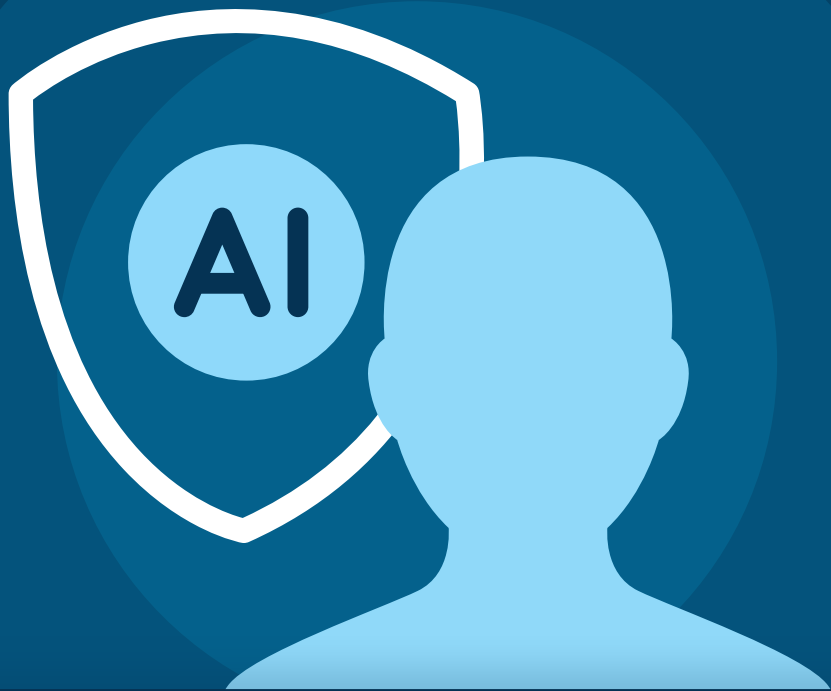


Katie
Elliott

Especially for BEC, the volume at which fraudsters can wreak havoc now because of AI is significant. You're casting a net and you're hoping someone's going to bite, and the more people a fraudster can send this bait out to, the more likely it is that someone's going to fall for it.

What happens when you're successful and get access? It's a time-consuming process to get into an email, but once they're in, now an AI agent can scrape that data, find messages from the CEO or that have procedures, and give you a one-pager.





Fighting Back Against AI Fraud with a Layered Approach

“It’s going to be a fight fire with fire approach,” Albert Laino says about AI fraud. That means using AI as a countermeasure is going to become critically important for fraud prevention practitioners.

What does that mean in practice? It means embracing AI’s powers to battle bad actors, while balancing the need to rely on ethically validated models rather than just the technology.



HOW TO USE AI TO BEST DETECT TODAY'S FRAUD SCHEMES

Laino notes that banks and fraud practitioners have guardrails and limitations with AI that fraudsters do not have, which increases the degree of difficulty of using it well.



However, banks, business payments networks, and businesses alike can use AI-enabled fraud solutions for real-time transaction and data analysis. These solutions help uncover deepfakes and odd behaviors, and flag and escalate those warning signs for experts to review.

AI is best positioned, to do analysis and find issues at a speed and scale humans simply cannot. For example, AI's pattern recognition capabilities mean it can analyze all login attempts for a platform and determine in seconds how many seem suspicious based on devices used, locations attempts are coming from, and other outlier behavior.

The human in the loop is there to take AI-generated data and make the best possible decision within an organization's guidelines, which in this example may involve informing a customer that they need to reset a password or closing off access to a potential fraudster.

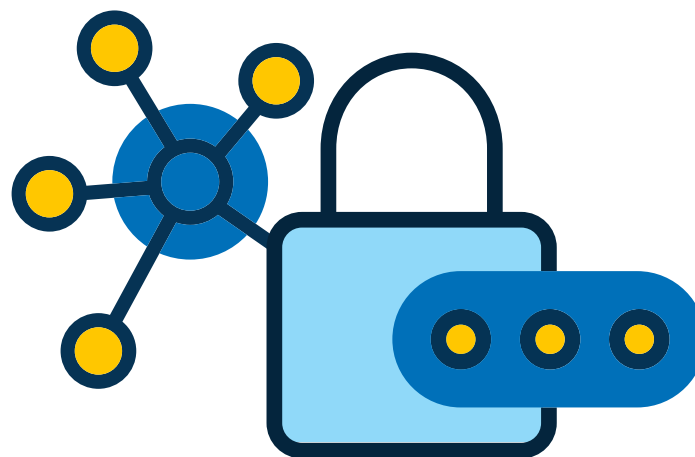


VERIFYING PAYMENTS AND ACCOUNTS, BOTH WITH AND WITHOUT AI

AI can be extremely helpful in recognizing suspicious patterns, especially with attempts to access accounts via brute force. Machine learning models should already be in place to help find those attempts before they become problematic. AI can also spot the warning signs of a spoofed email, like a “1” instead of an “l”, much more reliably than a human.

Layers are important, though, as Elliott notes.

A layered approach means having technology like multi-factor authentication, stringent checks on businesses enrolling to receive payments, and 24/7 monitoring for payment red flags. AI can enhance all three of those layers, but for many businesses it’s not yet accessible as a regular part of their technology stack. Classic fraud prevention techniques like MFA and strong passwords are still quite effective against most kinds of fraud, should the AI-enabled fraud prevention measures not be in place.





USE STRONG CONTROLS AND TRAINING TO PREVENT FRAUD

At the end of the day, all banks and businesses are as vulnerable to fraud as their least-trained employees. Those workers who feel pressure and don't stop to ask whether the request is legitimate, who don't know the warning signs of deepfakes and BEC, and are prone to blindly relying on AI and other technology to spot fraud are prime vectors for incidents to occur.

79% of businesses believe the finance team has a key role in preventing fraud

Instituting strong internal controls can help prevent any one employee from needing to make decisions that lead to fraud. Elliott recommends implementing dual controls and segregation of duties, where multiple approvers or multiple failsafes are present before any payment is made or account changes are allowed.

Furthermore, businesses must prioritize in-house training, making expert courses available when possible, and providing access to up-to-date tips and tricks on fraud avoidance from the experts via podcasts, videos, articles, and blog posts. An employee who knows deepfakes exist and knows what warning signs to look for will be far more likely to slow down and question an oddly phrased account change request from the CFO.





THE FRAUD EXPERTS POINT OF VIEW

Albert Laino

Where we're going to see AI being used to fight fraud effectively is really in the augmentation of what's existing today.

AI can enhance the signal quality of these rules-based systems, help with alert prioritization, and reduce investigation noise.

No one is saying let's create this all-knowing black box out there that's not going to enable fraud and prevent it from moving.

Banks and fraud practitioners want a tool to add enrichment and a layer on top that helps direct them on what to look at. Human intervention is still what they want for their most important investigations that bubble up to the surface.





THE FRAUD EXPERTS POINT OF VIEW



Katie Elliott

You can't rely on one piece of data. That means, you can't just rely on AI or any one check to say that this payment or payment instruction is good or bad.

There should be a dual process to help prevent AI fraud, one that involves technology and human expertise. That is important, that segregation of duties, the approvals, all of that will help to combat fraud.

Your business is helping people with a specific need, not preventing payment fraud. That's really our purpose here at Bottomline and my full-time job. Knowing where you want to spend your time and money to help you fight fraud is crucially important.





What Businesses Must Know **about AI Fraud**

AI-enabled fraud is everywhere, growing in scale and sophistication, and cannot be ignored. Fraudsters now have all the incentives in the world to use AI to help them with their schemes, given that they can do so much more efficiently and potentially with better results.

"A 1% success rate on a bigger number will ultimately get you more money at the end of the day. AI is giving bad actors the ability to scale, focus, and target how they interact with specific individuals. This gives them more opportunities to put their hooks into users and then ultimately, they facilitate these money movements," Laino said. "AI is going to be prevalent and just get better and better in that regard."

Knowing what kind of schemes are out there and what AI tools are available to help you fight them matters a great deal. As Elliott said, a balanced approach to fighting AI fraud will yield the best results.

"I think AI can be useful when you have large data sets that you need to sift through. You're looking for the needle in the haystack because transactions happen billions and trillions of times a day. I do think AI can be helpful for sorting and helping you escalate, but there always needs to be that human intervention and that human review," Elliott said.



TEST YOUR AI FRAUD KNOWLEDGE



0-2 Points:

Nice Try, Fraud Fighter Time for a quick refresher.

3-4 Points:

Fraud Savvy. You've got solid instincts.

5 Points:

AI Fraud Expert. You'd make a fraudster nervous.

1. What is a deepfake?

A rare fish found in the Mariana Trench

Fake internal messages posing as IT

AI-generated media that mimics a real person

Fake invoices sent to trick payment teams

2. With AI fraud, you're only as secure as your...

AI Tools

Vendors

Fraud Prevention Software

Least-Trained Employee

3. What's the best method to fight account takeovers?

Verify website URLs before entering credentials

Limit account access and monitor login activity

Watch for phishing emails and suspicious messages

Use all of these security practices

4. What are the two factors AI helps fraudsters solve for?

Cost and staffing needs

Credibility and scale

Time and human error

Account access issues

5. AI fraud is everywhere, so it's best to focus your efforts on...

Fighting AI with more AI

Reading every email with suspicion

Double-checking payments by phone

Layered defenses and expert support

TOTAL SCORE:

SHOW ANSWERS

HIDE ANSWERS





Fraud Prevention Methods to Remember

- **AI-Aided Prevention:** Use AI to keep an eye on networks, accounts, and suspicious behavior and rely on it to analyze reams of data and surface red flags and patterns that call for expert intervention.
- **Partner with Professionals:** Your own expert(s) should liaison with partners whose job it is to fight fraud, be they financial technology providers, dedicated fraud prevention specialists, or agentic AI builders.
- **Train and Encourage Your Team:** Your own team should know how to look for fraud warning signs and who to approach with those flags, and they should be encouraged to report suspicious items and to slow down when they feel pressure or sense that something is “off.” For every legitimate request that suffers a slight slowdown, a well-trained employee can prevent thousands of dollars and thousands of hours spent mitigating fraud losses.
- **Have Experts In-House:** You should have employees who understand what AI can do and what common types of fraud look like. Empower these employees to work in tandem with your own AI tools to keep your bank or business safe.

There's no magic bullet for preventing AI fraud, just as there never has been one for check fraud and BEC. Instead, fighting today's sophisticated fraud will involve embracing AI's potential to spot suspicious behavior more easily, working with partners who have proven technology and know-how to keep customers safe, and using layered protection. This layered protection involves monitoring accounts, having stringent controls and payment enrollment processes, and training and employee empowerment.

Banks and businesses must evolve to avoid AI-enabled fraud, because the cost of not getting it right is high. Adding protection to business payments—and ensuring customers are protected—is a rock-solid place to start, given that online banking and payments are a prime target for a new wave of fraudsters. Using the strategies we've outlined in this guide and working with partners that offer secure banking and business payments networks can help you get—and stay—ahead of AI fraud.



**Secure Your Accounts
with Digital Banking**



**Explore the Secure
Paymode Network**



REV US102126KV

© Copyright 2015 - 2026 Bottomline Technologies, Inc. All rights reserved.

Bottomline, Paymode, and the Bottomline logo are trademarks or registered trademarks of Bottomline Technologies, Inc. All other trademarks, brand names or logos are the property of their respective owners.

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1 603-436-0700
Toll-free: +1 800-243-2528
info@bottomline.com

