
AI Is Giving the Wolves New Teeth

How artificial intelligence is lowering the barriers to fraud, strengthening criminal organizations, and enabling a new generation of adversaries

David Haberland and Stephen Partello

SecureFi, Inc. | October 2026

The threat already in front of us

Much of today's conversation about artificial intelligence focuses on what might happen in the future.

Will AI eliminate millions of jobs? Will machines become more intelligent than humans? Could artificial intelligence eventually pose an existential threat?

Those questions deserve attention. But while much of the world debates what artificial intelligence might become, another threat is unfolding right in front of us.

AI is making fraud faster, cheaper, more convincing, and accessible to more people than ever before.

We think of criminals and malicious adversaries as the wolves. Some are sophisticated organizations operating across international borders. Others are individuals who recognize an opportunity to exploit someone else's trust.

Artificial intelligence is strengthening the established wolves while lowering the barriers for new ones to emerge.

This is not a theoretical concern about what AI might do decades from now. It is a growing challenge for consumers, businesses, financial institutions, and governments today.

Each of us brings more than 30 years of experience spanning technology, cybersecurity, intelligence, data, security, business operations, and commercial and federal markets. Throughout our careers, we've seen how adversaries adapt to technological advances, exploiting new capabilities to reduce costs, expand their reach, and increase their effectiveness.

Artificial intelligence is accelerating that process in ways that demand attention.

The economics of fraud are changing

Consider the barriers that traditionally constrained certain types of fraud.

Creating convincing communications required language skills. Building fraudulent websites required technical expertise or financial resources. Producing believable identities and supporting documents took additional effort. Researching potential victims and personalizing communications consumed time.

Those barriers have not disappeared, but they are falling.

Today, AI can help someone with limited writing skills generate professional correspondence in seconds. It can assist with website development, fabricate images, produce convincing documents, translate communications, and support increasingly sophisticated impersonation attempts.

The FBI documented these capabilities in December 2024, warning that criminals were exploiting generative AI to increase the believability and scale of financial fraud.

The advisory specifically identified AI-assisted translations that reduce grammatical errors by foreign criminal actors, faster production of fraudulent messages, fabricated identification documents, voice cloning, and generated videos used to impersonate authority figures.

In September 2026, the FBI issued another warning describing criminals using AI to appear as law enforcement and government officials during video calls.

These are documented capabilities and criminal techniques, not speculation.

The implications extend beyond the individual examples.

An adversary who previously needed several people to develop credible communications may now accomplish portions of that work with AI assistance. An operation that once relied on generic messages can produce more personalized approaches. A criminal who struggled to appear legitimate can create increasingly convincing material.

This is especially significant when viewed through the economics of criminal activity.

AI can reduce the cost of producing fraudulent content, shorten the time required to prepare an attempt, and increase the number of potential victims an operation can approach.

It can also make experimentation easier. Fraudsters can revise their communications, refine their impersonations, and adapt their approaches without necessarily requiring the specialized resources previously associated with such efforts.

Not every capability translates into a successful crime. Defenders are also adopting AI, and criminals continue to face technical, financial, and operational challenges.

Nevertheless, the underlying economics of deception are changing, and that changes the threat landscape.

The emergence of new wolves

The discussion about AI-enabled fraud often concentrates on sophisticated criminal organizations.

That focus is justified. Established fraud networks already possess infrastructure, experience, financial incentives, and access to victims. Increasing their productivity and sophistication can have serious consequences.

But we believe another development deserves equal attention.

OUR ASSESSMENT

Our assessment is that AI is lowering the barriers sufficiently to enable more inexperienced and opportunistic individuals to attempt fraud that previously required greater expertise, resources, or preparation.

This is an assessment of emerging capabilities, not a claim that researchers have already measured a corresponding increase in first-time fraudsters.

The reasoning is straightforward.

When specialized skills become easier to obtain, the population capable of attempting an activity can expand.

- Someone who could not build a convincing fraudulent website may now be able to create one with AI-assisted development tools.
- Someone who previously struggled to impersonate a business may be able to produce professional communications, branding, and supporting materials.
- Someone with little experience in deception can experiment with fake job offers, false identities, or fraudulent payment requests using tools that help improve the credibility of the presentation.

This is a meaningful change in accessibility.

Historically, certain forms of fraud required technical knowledge, organizational infrastructure, financial investment, or access to specialized services.

AI does not eliminate those requirements entirely, but it can make portions of the process much easier.

That creates an opportunity for criminals who were previously constrained by their own lack of skills.

Some attempts will remain crude and unsuccessful. AI does not automatically provide criminal judgment, operational discipline, or the ability to evade detection.

But the cost of experimenting is falling.

That matters because the threat may no longer come primarily from established fraud organizations becoming more productive. It may also come from a wider population of less experienced participants who now have access to capabilities once beyond their reach.

We need to prepare for both.

When credibility can be manufactured

For years, consumers and employees were taught to identify suspicious communications by looking for familiar warning signs.

Poor grammar. Unusual phrasing. Unprofessional websites. Strange images. Inconsistent identities. A caller who did not sound quite right.

Those indicators remain useful, but they are becoming less reliable.

A fraudulent recruitment email can reference a real company and position, use professional language, and appear to come from an experienced recruiter.

A family emergency scam can incorporate a familiar voice.

A fabricated identity can include photographs, credentials, and supporting documents that appear authentic.

And criminals can exploit information that is entirely genuine to support an impersonation.

In September 2026, FBI Newark warned about criminals impersonating federal law enforcement agents using real agents' names and spoofed government telephone numbers.

Victims who contacted an agency to check the name of the purported agent sometimes learned that the agent genuinely worked there. That confirmation could create a false sense of legitimacy about the original caller, even though it did not establish that the caller was actually the agent.

In one reported incident, a fraudster used a virtual meeting platform and staged the background to resemble an FBI office, including a desk, an FBI seal, and a professionally dressed individual.

The criminals were not simply inventing identities. They were exploiting authentic information and familiar symbols of authority to make fraudulent communications more credible.

Importantly, the FBI Newark warning did not establish that the staged video meeting used AI. The example demonstrates how effective impersonation can become when criminals combine legitimate information with deceptive presentation, even without confirmed AI involvement.

AI can further expand the possibilities for creating convincing identities and communications.

These schemes do not all require artificial intelligence. Many existed long before generative AI became widely available.

What AI changes is the effort required to make them convincing.

The danger is not that every realistic communication is fraudulent or that every scam uses AI. It is that familiar indicators of authenticity are becoming easier for adversaries to reproduce.

We are moving toward an environment where recognizing a name, hearing a voice, or seeing a professional-looking document may tell us very little about whether the person behind it is legitimate.

Trust increasingly requires independent verification rather than appearances.

The consequences extend beyond the victim

The scale of existing fraud provides important context.

Research published in June 2026 by Gallup and the Stop Scams Alliance estimated that approximately 15 million American adults personally lost money to scams in 2025, with aggregate losses estimated at \$68 billion.

These figures describe the broader fraud problem, not losses specifically attributable to artificial intelligence.

The same research found that victims reported AI or deepfake involvement in approximately 12% of successful scams experienced during 2025.

That number needs careful interpretation.

It reflects what victims recognized or reported, not an independent technical determination of whether AI was involved. Some victims may have been unaware that AI played a role, while others may have attributed sophisticated deception to AI without being able to verify it.

The finding should not be interpreted as evidence that AI caused 12% of total fraud losses.

Nevertheless, it provides a useful indication that consumers are already encountering fraud they perceive as involving AI-generated or manipulated content.

The actual extent of AI involvement remains difficult to measure.

And the consequences of fraud extend well beyond the reported financial losses.

Fraud can devastate retirement savings, household finances, and small businesses. It can create embarrassment, isolation, anxiety, and lasting distrust.

But there is another consequence that receives less attention.

As impersonation becomes easier, legitimate organizations face growing difficulty establishing trust with the people they serve.

- Banks must distinguish genuine customers and payment instructions from impersonation attempts.
- Employers must contend with fraudulent recruiters using their names.

- Government agencies may discover that criminals are exploiting their identities, authority, and public communications.
- Businesses must verify suppliers, invoices, executives, and unexpected requests.
- Families must consider whether a familiar voice or urgent message is authentic.

Even when an organization has done nothing wrong, its reputation can be used against the people who trust it.

The resulting uncertainty imposes costs on everyone. Legitimate interactions become harder, verification consumes more time, and people may become reluctant to engage with communications they once accepted without question.

Fraud is no longer just a matter of stolen money. It is increasingly a challenge to trust across the digital economy.

The defenders must adapt

We cannot solve this problem solely by telling people to be more careful.

Consumers should remain skeptical of unexpected requests, but expecting every person to identify sophisticated AI-enabled deception is unrealistic.

The response must reflect the changing capabilities of the adversaries.

- Technology providers need to strengthen safeguards against misuse.
- Financial institutions need effective authentication and intervention processes, particularly when suspicious requests involve transferring money or changing account access.
- Businesses and government agencies need practical ways for people to independently verify their communications.
- Law enforcement and regulators need stronger coordination, timely threat information, and mechanisms for identifying recurring patterns across jurisdictions and organizations.
- And consumers need access to understandable guidance before and after an incident.

These are connected responsibilities.

The defensive challenge is not simply to detect AI-generated material. A legitimate-looking communication may be fraudulent without using AI at all. Conversely, legitimate organizations increasingly use AI in their normal operations.

The more important question is whether the identity, authority, transaction, and requested action can be trusted.

That requires approaches centered on risk and verification rather than appearance alone.

Prevention is only the beginning

Fraud prevention receives much of the attention, but preventing every incident is not realistic.

A credible response must address the complete lifecycle.

- Help someone recognize a potential threat before acting.
- Provide a way to verify the person, organization, or request independently.
- When harm occurs, help the victim protect accounts, contact the appropriate institutions, preserve evidence, and understand available recovery options.
- Make reporting easier and more useful.

With appropriate legal authority, privacy protections, and consent, information from incidents can contribute to identifying emerging fraud patterns. Those patterns can inform warnings, defensive improvements, and future prevention efforts.

This connected approach matters because individual incidents may reveal something useful about a broader threat.

At SecureFi.AI, this thinking is central to our work around personal risk intelligence, verification, recovery, reporting, and threat awareness.

The objective is not to replace banks, law enforcement, or government agencies. It is to help individuals make more informed decisions and navigate the organizations and processes that can assist them.

AI can play an important role in that effort. The same broad technological advances that criminals exploit can also help defenders analyze suspicious communications, correlate threat information, and provide guidance at scale.

The challenge is ensuring defensive capabilities become accessible and useful to ordinary people, not just large institutions.

For consumers, two habits remain especially important.

First, independently contact an organization or family member through a trusted channel before responding to an unexpected request, especially one involving money, sensitive information, or security codes.

Second, recognize urgency as a reason to verify, not a reason to bypass verification.

If money or information has already been shared, contact the relevant financial institution immediately, secure affected accounts, preserve the evidence, and report the incident through appropriate official channels.

A different kind of AI challenge

We believe artificial intelligence has enormous potential to improve healthcare, education, research, productivity, cybersecurity, and everyday life.

We are not arguing against its development or adoption.

We are arguing that its benefits and its potential for criminal exploitation must be considered together.

The challenge for defenders is substantial because AI does not merely introduce new fraud techniques. It can improve existing ones while expanding access to the capabilities needed to attempt them.

- Established criminal organizations may become more efficient.
- Experienced fraudsters may become more convincing.
- Opportunistic individuals may gain the confidence and means to attempt schemes they previously could not execute.

Meanwhile, consumers and organizations must operate in an environment where familiar signals of legitimacy are increasingly easy to imitate.

We should not wait for definitive statistics proving that every aspect of this threat has accelerated before responding to capabilities that are already documented.

We need stronger verification, more accessible protection, better coordination, and a response that connects prevention with recovery, reporting, and intelligence.

The real question is whether our defenses can adapt quickly enough as the barriers to deception continue to fall.

The wolves don't need artificial intelligence to become conscious.
They just need it to become useful.

About the Authors

David Haberland is the Founder of SecureFi, Inc., with more than 30 years of experience in technology leadership, cybersecurity, data, intelligence, and commercial and public sector markets.

Stephen Partello is Legal Counsel and Director of Operations for SecureFi, Inc., with more than 30 years of experience spanning legal affairs, contracts, business operations, and commercial and federal markets.

Together, they bring complementary perspectives on emerging technologies, adversarial threats, organizational risk, and the evolving challenges of fraud prevention.

Sources and References

1. **Federal Bureau of Investigation, Internet Crime Complaint Center.**
[*Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*](#) December 3, 2024.
Documents criminals' use of generative AI to produce fraudulent communications, improve translations, create fictitious identities, clone voices, and generate deceptive audio and video.
2. **Federal Bureau of Investigation, Internet Crime Complaint Center.**
[*Scammers Impersonating Law Enforcement and Government Officials in Fraud Schemes*](#) September 17, 2026.
Describes government and law enforcement impersonation schemes, including the use of AI to create convincing appearances during video calls.
3. **Federal Bureau of Investigation, Newark Field Office.**
[*FBI Newark Issues Warning About Insidious New Twist on an Old Fraud Scheme*](#) September 29, 2026.
Documents impersonation involving real federal agents' names, spoofed government telephone numbers, and staged video meetings designed to resemble official settings.
4. **Gallup and Stop Scams Alliance.**
[*United States of Scams: The Financial and Emotional Fallout*](#) June 2026.
Research on the frequency, financial losses, emotional consequences, and reported characteristics of scams affecting American adults.
5. **Gallup.**
[*Scam Victims Report Billions Lost and Harm to Mental Health*](#) June 29, 2026.
Summarizes findings on the financial and emotional consequences of scams.

The analysis presented in this article reflects the authors' perspectives on emerging technology and fraud risk. Observations concerning the potential expansion of opportunistic fraud are forward-looking assessments based on changing technological capabilities, rather than established statistical findings.