

tip411 Highlights Strong Security Protections Following Reports of Breach Impacting Other Anonymous Tip Platforms

MN, UNITED STATES, April 14, 2026 /EINPresswire.com/ -- While [tip411](#)'s systems were not breached or affected, recent national reporting about a [cybersecurity](#) incident affecting millions of anonymous crime-tip records in P3 Global Intel and its Crime Stoppers clients has raised important questions about how agencies protect sensitive information submitted by the public.



tip411 – a leading anonymous tip platform used successfully in over 2,500 communities across the U.S. – is reaffirming its long-standing commitment to privacy-first system design and continuous cybersecurity monitoring and highlighting the platform's use of a FedRAMP

Moderate-authorized cloud environment to strengthen protections for agencies and tipsters.

“

Anonymous reporting systems only work if the public trusts them. Our responsibility is to make sure agencies—and the communities they serve—can rely on the protections built into tip411.”

*Terry Halsch, President of
tip411*

“Systems that collect sensitive community information must be designed with security as a continuous process—not a one-time setup,” said Terry Halsch, President of tip411.

Due to the increasing risk of cyber attacks, tip411 has taken additional steps to safeguard its customers' data. As part of its proactive cybersecurity strategy, tip411 migrated its hosting infrastructure to an Amazon Web Services (AWS) FedRAMP Moderate environment in April 2023, meeting federal standards for handling sensitive data. FedRAMP

Moderate requires strong protections for encryption, access control, monitoring, and continuous security oversight.

FedRAMP (the Federal Risk and Authorization Management Program) establishes standardized security requirements for cloud systems used by federal agencies and contractors. A Moderate authorization level means the system meets rigorous standards for:

- data protection safeguards
- access control and authentication

- encryption and secure system architecture
- vulnerability monitoring and response
- continuous security oversight and auditing

Unlike some legacy or third-party-dependent anonymous reporting infrastructures, tip411 was built specifically to support secure two-way anonymous communication between the public and law enforcement while minimizing the collection of identifying information.

Security-focused design features include:

- true two-way anonymous messaging without requiring tipster identity disclosure
- minimal data-collection architecture that reduces exposure risk
- encrypted communications pathways
- agency-controlled deployment environments
- continuous monitoring aligned with federal cloud security standards
- infrastructure hosted within a FedRAMP Moderate AWS environment

Together, these protections help agencies maintain trusted communication channels with community members while safeguarding the privacy expectations that make anonymous reporting effective.

“Anonymous reporting systems only work if the public trusts them,” Halsch said. “Our responsibility is to make sure agencies—and the communities they serve—can rely on the protections built into tip411.”

For more information about tip411’s secure anonymous reporting platform, visit www.tip411.com.

Terry Halsch

Citizen Observer

+1 315-481-3490

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/905336597>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

