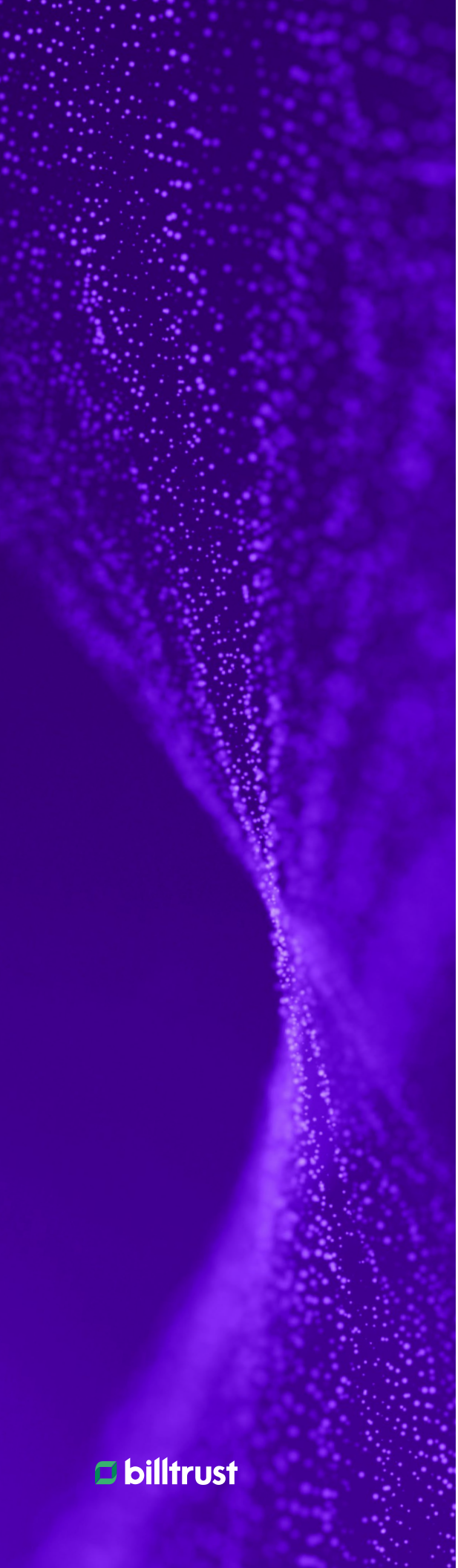
billtrust

WHITE PAPER

Smart moves: Why AI will revolutionize the fight against cyber fraud



billtrust

Cyber fraud is rampant. Can AI help?

With the rise of generative AI, artificial intelligence continues to take the world by storm, constantly evolving and filtering into new market segments.

Key among these is the field of cybersecurity. Forward-looking companies are harnessing the power of AI in the fight against cyber fraud to identify and respond to cyber threats in real time, potentially saving businesses billions of dollars.

Last year, cybercrime cost U.S. businesses more than $10 billion[1], according to the 2022 Internet Crime Report produced by the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3). What's more, predictions are placing global damage at a staggering $10.5 trillion annually by 2025, according to Cybersecurity Ventures.[2]

"This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined," says Cybersecurity Ventures[3].

Billtrust customers are anxious about payments fraud. One customer recently said, "I've talked to some ... folks that have had people listen in on earnings release calls and record those to get the computer to learn the cadence of speech and tone to where they can use AI tape technology, call a finance person, leave them a voicemail in the voice cadence of your CFO or someone else saying, 'Hey, I need you to send this money to XYZ.' And you can hardly tell the difference."

The high cost of cyber fraud

$343B: Predicted global losses to businesses due to online payments fraud between 2023 and 2027[4]

$4.45M: The global average cost of a data breach in 2023, a 15% increase over 3 years[5]

$955K: The cost to small and mid-sized businesses of restoring normal business after successful cyberattacks[6]

The unintended consequences of digitization

In the wake of the pandemic, businesses changed their business models, moving toward the greater digitization of products and services and resulting in an explosion of sophisticated cybercrimes.

According to PwC's Global Economic Crime and Fraud Survey 2022, today's predator is more likely to prey on a business's vulnerabilities using sophisticated schemes and tactics that even a year or two ago were not available[7]. The tools of yesterday fail to meet the cyber challenges of today. It's that simple.

Billtrust is committed to AI

Cybercrime and its cost to businesses is skyrocketing. That's one reason Billtrust is committed to empowering chief financial officers (CFOs) to be leaders in their organizations, which means ensuring they understand how to protect the bottom line. We do that by giving companies access to data gathered through automation and machine learning to detect fraud better and help reduce human error.

Bottom line? Billtrust is arming finance teams with information that not only improves their ability to detect fraud but also gives them more time to guard against it.

Billtrust has a systematic approach to AI that sets the foundation for future innovation, keeping data security and privacy top of mind. We offer cross-product analytics, generative AI for intuitive queries, and personalized alerts, revolutionizing data-driven decision-making and customer communications.

Billtrust is committed to data security

Understandably, many people are concerned about the security of financial data and implications of using that data in AI applications. At Billtrust, data security and usage is top of mind. Here are some common concerns.

Q: Where does Billtrust store AR data?

A: In addition to accessing and sharing data, an equally crucial aspect of data security is data storage. Billtrust's product engineer teams are composed of engineers, product owners, designers, analysts, and technical leaders who are focused on building solutions. We are a cloud-first development organization, using design-centered thinking. We store data in cutting-edge cloud solutions like Snowflake and MongoDB. Both are equipped with robust built-in security and governance features.

Q: How does Billtrust protect sensitive information and data?

A: Generative AI chats can't do without sharing data and information, but when Billtrust uses these large language models (LLMs), we make a commitment to keeping data private. For data analysis purposes, only the structure of data tables, schemas, and data definitions are transmitted. Billtrust adheres to stringent policies that expressly prohibit the utilization of shared data for external training or any purposes outside the scope of our products and services.

Q: What AI models or plans does Billtrust use?

A: We leverage OpenAI Enterprise or Azure OpenAI, whose data usage policies are compliant with our existing mandates with our customers. We will never share personal identifying information (PII) or credit card data. Additionally, no data shared with a third party will ever be used for external training or for other use cases outside the boundaries of Billtrust products and services.

5 fraud trends to watch out for

Against this evolving cyber fraud backdrop, several types of cyber risks stand out. Michelle Moore, PhD, Director of Graduate Cyber Security Operations and Leadership and professor of practice with the University of San Diego, points to these top trends and threats in cyber fraud:

1. Data breaches:
Moore says that according to Comparitech, the U.S. has experienced the most data breaches with 212.4 million people affected in 2021 (compared with 174.4 million in 2020)[8]. What's more, companies that experience a data breach underperform the market by more than 15% three years later.[9]

3. Ransomware:
Like other forms of cyber fraud, ransomware strategies continue to evolve, costing victims billions of dollars annually. Moore explains that these cyber-attacks "kidnap" an individual's or organization's databases, holding all the information for ransom.

4. Business email compromise (BEC):
Also known as payment diversion fraud, BEC occurs when a legitimate email account is either compromised or impersonated and used to fraudulently order or request the transfer of funds to a third party.

5. Cloud infrastructure compromise:
Cloud service providers add another layer of vulnerabilities to businesses as hackers exploit the numerous vulnerabilities, resulting in widespread compromises of multiple databases and applications.

> **"I've signed six [check fraud] declaration forms this month. ... I haven't really signed that many in my two years as a cash application manager. But yeah, it's just intercepting checks. You're talking about AI and the phishing emails are getting better and better and better. I think it wasn't on us, but a customer got called in a phishing scam, owed us a large balance. They sent $400,000 to this fraudulent account, not able to recover it. They still owe us the money."**
>
> — Billtrust customer

By the numbers: Business email compromise

277,918

The number of domestic and international BEC incidents

$50.9B

Domestic and international exposed dollar loss from BEC

Source: FBI Public Service Announcement, June 9, 2023

Cyber fraud prevention and detection: AI to the rescue

With the growing complexity of cyber fraud and the sophistication of cybercriminals, AI will be a game changer in the fight against cyber fraud. AI-enabled fraud detection and prevention solutions are poised to revolutionize cybersecurity because of the breadth and depth of their capabilities, coupled with unrivalled speed.

Let's look at a few of these amazing capabilities:

- **AI can analyze vast amounts of data:** One of the many advantages of AI is its ability to analyze "vast amounts of data in real time, identifying patterns and anomalies to flag potential fraudulent activities9," explains fraud.com.

- **AI can stop threats before they materialize:** "AI learns with historical data and can adjust its rules to stop threats it may have never seen before—something standard fraud software cannot do," explains Data Dome.10 "Because AI is dynamic, it also continuously works to reduce the number of false positives (genuine users being blocked) by improving the accuracy of its rules."

- **AI saves time and money:** At Billtrust, we've started to incorporate AI and machine learning in some of our products, and we're constantly monitoring tools and frameworks that make the daily lives of CFOs and AR teams a lot simpler by enhancing team efficiency. Essentially, AI frees up your team to focus on fraud detection.

- **AI reduces human error and risk:** According to Verizon's 2022 Data Breaches Investigations Report, 74% of all data breaches involve a human element, including errors, database mistakes, exposing information, and more. These tools help eliminate the human element, reducing data breaches and other cyber risks.

AI fraud is getting more sophisticated. Are your finance team's operations?

Although no one can predict with certainty how AI fraud detection and prevention solutions will evolve in the months and years ahead, it is safe to say they will become increasingly sophisticated. With a heightened capacity to apply more complex algorithms to data, businesses can expect faster and more accurate cyber fraud detection.

At Billtrust, we're committed to harnessing the power of AI to provide our customers with the data they need in the fight against cyber fraud.

"We offer an AI-powered, complete view of customers' activity across your entire AR process, enabling you to make intelligent AR decisions," says Ahsan Shah, Billtrust Senior VP Data Analytics.

References

1. Federal Bureau of Investigation, "Internet Crime Complaint Center Releases 2022 Statistics," March 22, https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics.
2. Cybersecurity Ventures," Cybercrime to Cost the World $10.5 Trillion Annually by 2025," https://www.prnewswire.com/news-releases/cybercrime-to-cost-the-world-10-5-trillion-annually-by-2025--301172786.html.
3. Ibid
4. Juniper Research, "Online Payment Fraud Losses to Exceed $343 Billion Globally Over the Next 5 Years, Juniper Research Study Finds," July 11, 2022, https://www.juniperresearch.com/pressreleases/online-payment-fraud-losses-to-exceed-343bn.
5. IBM, Cost of Data Breach Report 2023, https://www.ibm.com/reports/data-breach.
6. ARF Financial, "Scary Cybersecurity Facts for Small Business Owners," https://www.arffinancial.com/scary-cybersecurity-facts-for-small-business-owners/#:~:text=But%20the%20costs%20of%20recovering,is%20stolen%20from%20these%20businesses.
7. PWC, Global Economic and Crime Survey 2022, https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC's-Global-Economic-Crime-and-Fraud-Survey-2022.pdf.
8. Comparitech, "30+ data breach statistics and facts," https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/#:~:text=According%20to%20statistics%20from%20Surfshark,from%201.4%20million%20in%202020).
9. Comparitech, "30+ data breach statistics and facts," https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/#:~:text=According%20to%20statistics%20from%20Surfshark,from%201.4%20million%20in%202020.

billtrust

Learn more

Visit billtrust.com or contact our sales team.

ABOUT BILLTRUST

Finance leaders turn to Billtrust to get paid faster while controlling costs, accelerating cash flow and maximizing customer satisfaction. As a B2B order-to-cash software and digital payments market leader, we help the world's leading brands move finance forward with AI-powered solutions to transition from expensive paper invoicing and check acceptance to efficient electronic billing and payments. With more than 2,400 global customers and more than $1 trillion invoice dollars processed, Billtrust delivers business value through deep industry expertise and a culture relentlessly focused on delivering meaningful customer outcomes.

CORPORATE HEADQUARTERS

11D South Gold Drive
Hamilton Township, New Jersey 08691
United States

SACRAMENTO

2400 Port Street
West Sacramento, California 95691
United States

GHENT

Moutstraat 64 bus 501
9000 Ghent
Belgium

AMSTERDAM

H.J.E. Wenckebachweg 200-III
AS 1096 Amsterdam
Netherlands

KRAKÓW

ul. prof Michała Życzkowskiego 19
3 piętro
Kraków 31-864
Poland

© 2024 BTRS Holdings Inc. dba Billtrust. All rights reserved. Billtrust and the Billtrust Logo are registered trademarks of Billtrust.

PM-BT-WP19-v1.1