Digital fraud is skyrocketing. And it's costing you.

Find out how contextual decisioning can help you move from detection to prevention and outsmart tech-savvy fraudsters.

teradata. | celebrus FRAUD DATA PLATFORM

COVID-19 accelerated consumer adoption of digital channels.

And fraudsters followed.

The digital fraud landscape at-a-glance

Digital fraud is on the rise. Fraudsters have quickly developed new strategies to exploit digital channels.

Losses are escalating. With the emergence of real-time payments, losses happen fast and the ability to recover is low.

Regulators are increasing pressure on banks to act. Detection and prevention have become a top priority for financial services.

91%
increase in scams in 2020[1]

5%
of all digital traffic is an account takeover attack[2]

$206B
in online fraud losses is predicted for 2021-2025[3]

1 Scam Advisor 'The Global State of Scams 2021'
2 Arkose Labs, "How Cybercriminals Hack into a Digital Account in a Few Easy Steps"
3 Arkose Labs, "Fake New Account Fraud Rose 70% in H1 2021"

But current fraud solutions are inadequate and lack sophistication to activate all data—both transactional and digital.

In a world of real-time digital payments, these solutions are falling behind.

Traditional fraud solutions are transactional and backward focused

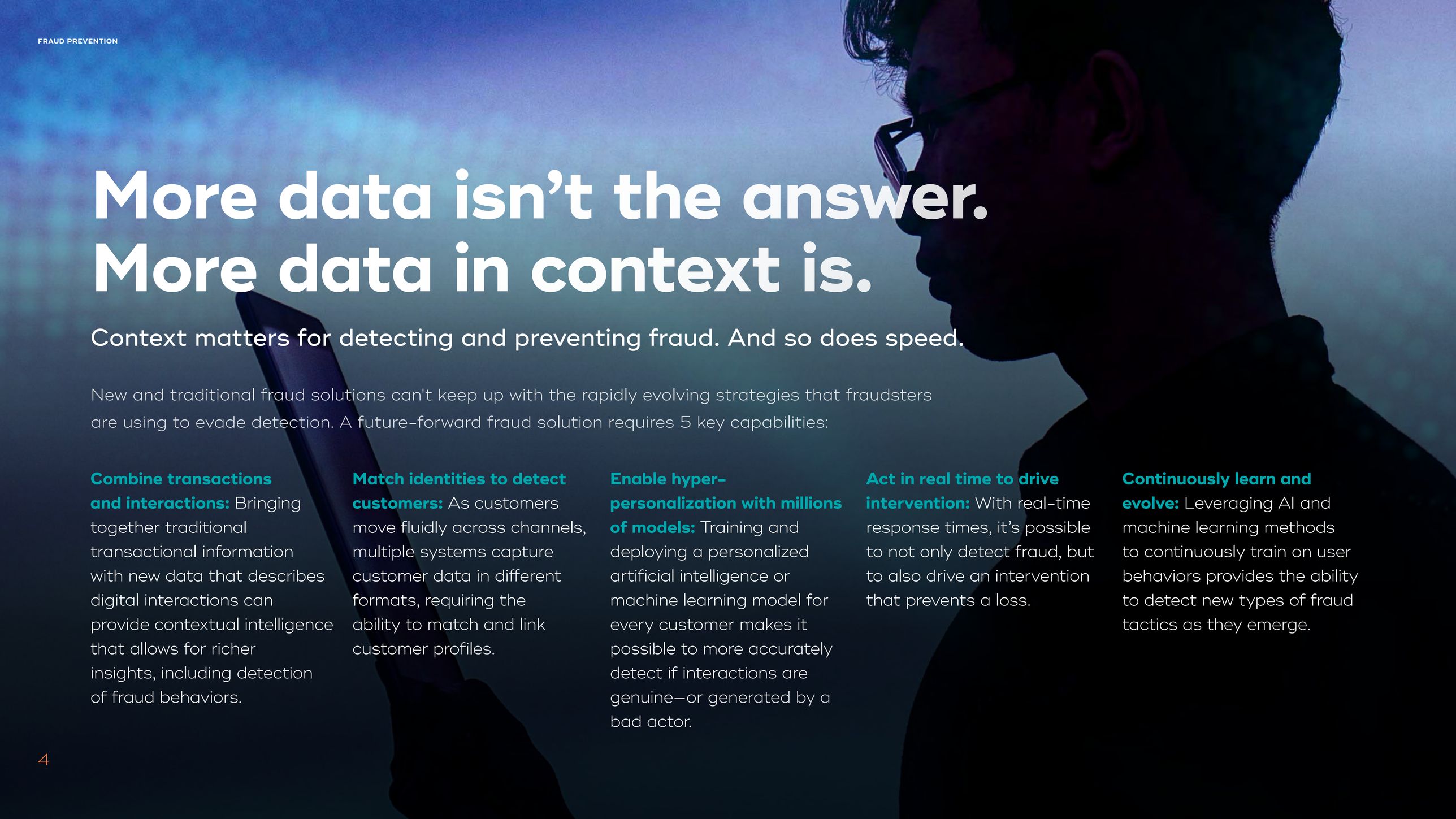
Traditional fraud solutions only focus on transactions and the historical transaction patterns. These solutions ignore behaviors detected around each transaction and instead rely on decisioning rules that are **rigid and difficult to adapt.**

Newer fraud solutions only focus on behavioral detection and are often black box

Newer solutions offer behavioral biometrics analysis, but don't incorporate transactional knowledge. These solutions are **low in precision and accuracy and typically lack explainability.**

Both new and traditional solutions are reactive, not preventative

The majority of fraud solutions, both new and traditional, provide capabilities to detect and investigate fraud after it has happened, but **are unable to prevent fraud in real time.**



More data isn’t the answer. More data in context is.

Context matters for detecting and preventing fraud. And so does speed.

New and traditional fraud solutions can't keep up with the rapidly evolving strategies that fraudsters are using to evade detection. A future-forward fraud solution requires 5 key capabilities:

Combine transactions and interactions: Bringing together traditional transactional information with new data that describes digital interactions can provide contextual intelligence that allows for richer insights, including detection of fraud behaviors.

Match identities to detect customers: As customers move fluidly across channels, multiple systems capture customer data in different formats, requiring the ability to match and link customer profiles.

Enable hyper-personalization with millions of models: Training and deploying a personalized artificial intelligence or machine learning model for every customer makes it possible to more accurately detect if interactions are genuine—or generated by a bad actor.

Act in real time to drive intervention: With real-time response times, it’s possible to not only detect fraud, but to also drive an intervention that prevents a loss.

Continuously learn and evolve: Leveraging AI and machine learning methods to continuously train on user behaviors provides the ability to detect new types of fraud tactics as they emerge.

It’s time to switch from detection to prevention.

To stop fraud, you need a solution that enables you to understand bad actors and intervene in their journeys with preventative action.

Listen by building a contextual view of each transaction, combining information about the transaction and digital behaviors that describe how a user is navigating, moving, and interacting within digital channels.

Understand the fraud risk by applying hyper-personalized AI and machine learning models, in real time, that both profile and compare an individual customer with their expected behavior.

Decide if an intervention is required and if so, determine the severity of intervention needed, thereby optimizing the trade-off between minimizing losses, maximizing customer experiences, and lowering the cost of fraud management.

Act by delivering the intervention in real time to prevent the fraud or allowing the transaction to proceed if it’s assessed as genuine.

Fraud Intervention Strategies

Probability of Fraud	Strategy	Intervention Measures
95%	Kick Intervention	Block the payment, pending investigation
70-95%	SMS Intervention	Fraud message and two-factor authentication requirement
50-70%	Manual Authentication by Fraud-Ops	Customer warning message followed by further investigation

Prevent fraud—at scale and in real time—with contextual decisioning.

With Teradata and Celebrus you can:

Reduce fraud losses by intervening in fraudulent transactions in real time

Reduce false positives and create better customer experiences by only stopping fraudulent transactions, not genuine ones

Improve the customer experience by proactively intervening to protect customers at risk

Eliminate overhead and improve efficiency by reducing fraud investigations and case management, as well as providing insights that simplify investigations

Address evolving threats while staying ahead of—and responding quickly to—new fraud types and strategies

CASE STUDY

Staying one step ahead of fraudsters to protect customers.

PROBLEM

A global top 5 bank was struggling with Remote Access Takeover (RAT) fraud, which was growing 15% during COVID. With losses and pressure from regulators escalating, the bank needed to act fast.

The bank needed a real-time solution to detect fraud and prevent losses before they happened.

2,000+
Fraud cases per month

$2,700
Loss per fraud case

SOLUTION

After deploying Teradata Vantage™ and Celebrus, the bank was able to establish a hyper-personalized behavioral fraud solution that could prevent fraud, improve the customer experience, reduce losses, and improve business efficiency by:

- Capturing digital interactions in real time
- Analyzing the data for transactional and behavioral patterns
- Running millions of micro models to assess behaviors
- Deploying insights in sub-second response times

250K
Unique customer journeys analyzed per hour at peak times

70%
Cases of fraud are now detectable and preventable

$100M
In preventable fraud detected

Deploying fraud prevention at scale is easy

with Teradata and Celebrus.

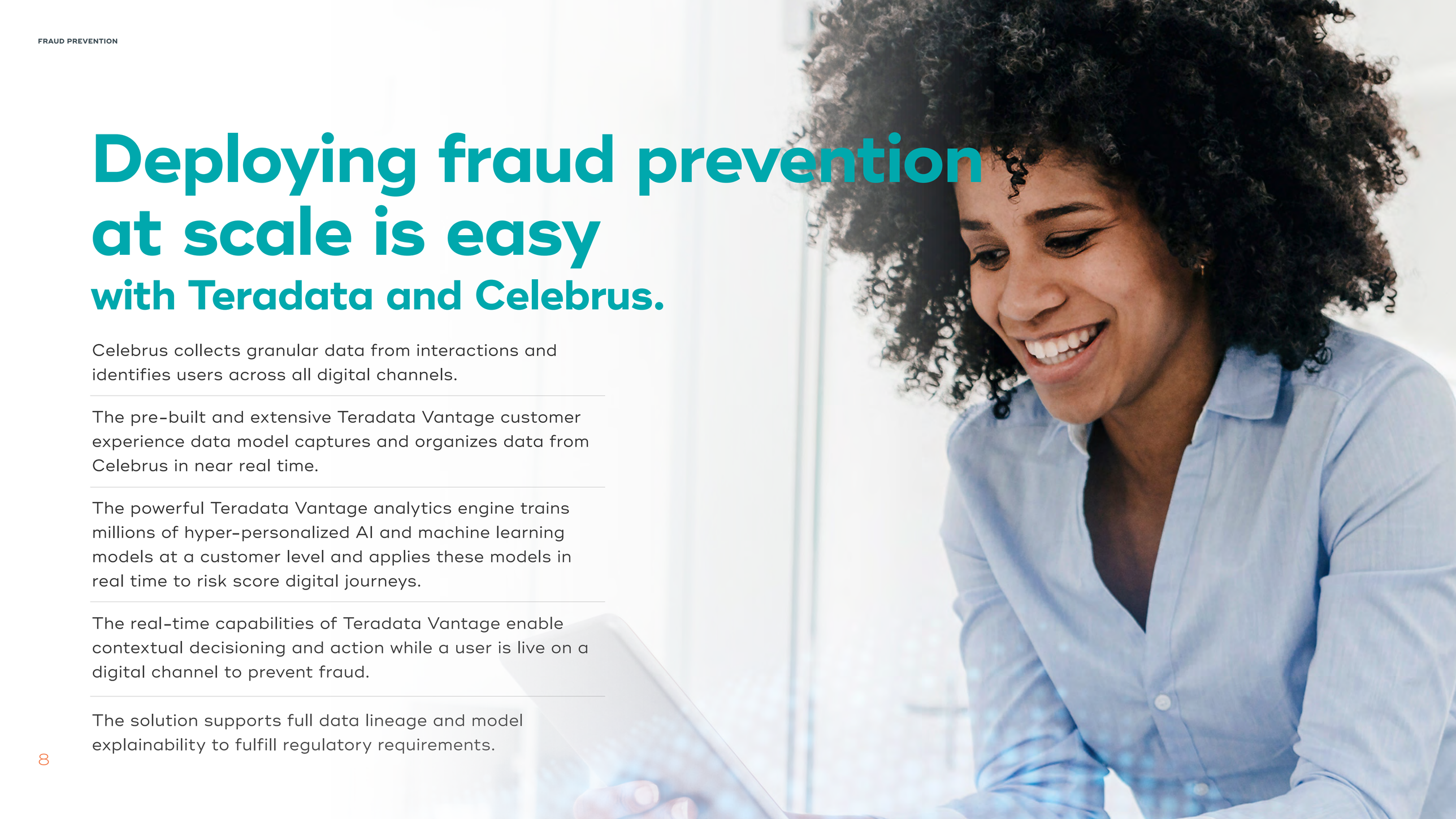
Celebrus collects granular data from interactions and identifies users across all digital channels.

The pre-built and extensive Teradata Vantage customer experience data model captures and organizes data from Celebrus in near real time.

The powerful Teradata Vantage analytics engine trains millions of hyper-personalized AI and machine learning models at a customer level and applies these models in real time to risk score digital journeys.

The real-time capabilities of Teradata Vantage enable contextual decisioning and action while a user is live on a digital channel to prevent fraud.

The solution supports full data lineage and model explainability to fulfill regulatory requirements.



Unlock the full potential of fraud prevention with the power of data.

Get the power, scalability, and enterprise analytics needed to enable fraud prevention from start to scale.

Celebrus is the world's only first-party, real-time, enterprise-class data capture and contextualization solution that unlocks huge savings and incremental online revenues, through the creation of world-class digital experiences for each online customer. **Learn more at Celebrus.com**

Teradata is the connected multi-cloud data platform for enterprise analytics company. Our enterprise analytics solve business challenges from start to scale. Only Teradata gives you the flexibility to handle the massive and mixed data workloads of the future, today. **Learn more at Teradata.com**

17095 Via Del Campo, San Diego, CA 92127 Teradata.com

teradata. | celebrus FRAUD DATA PLATFORM