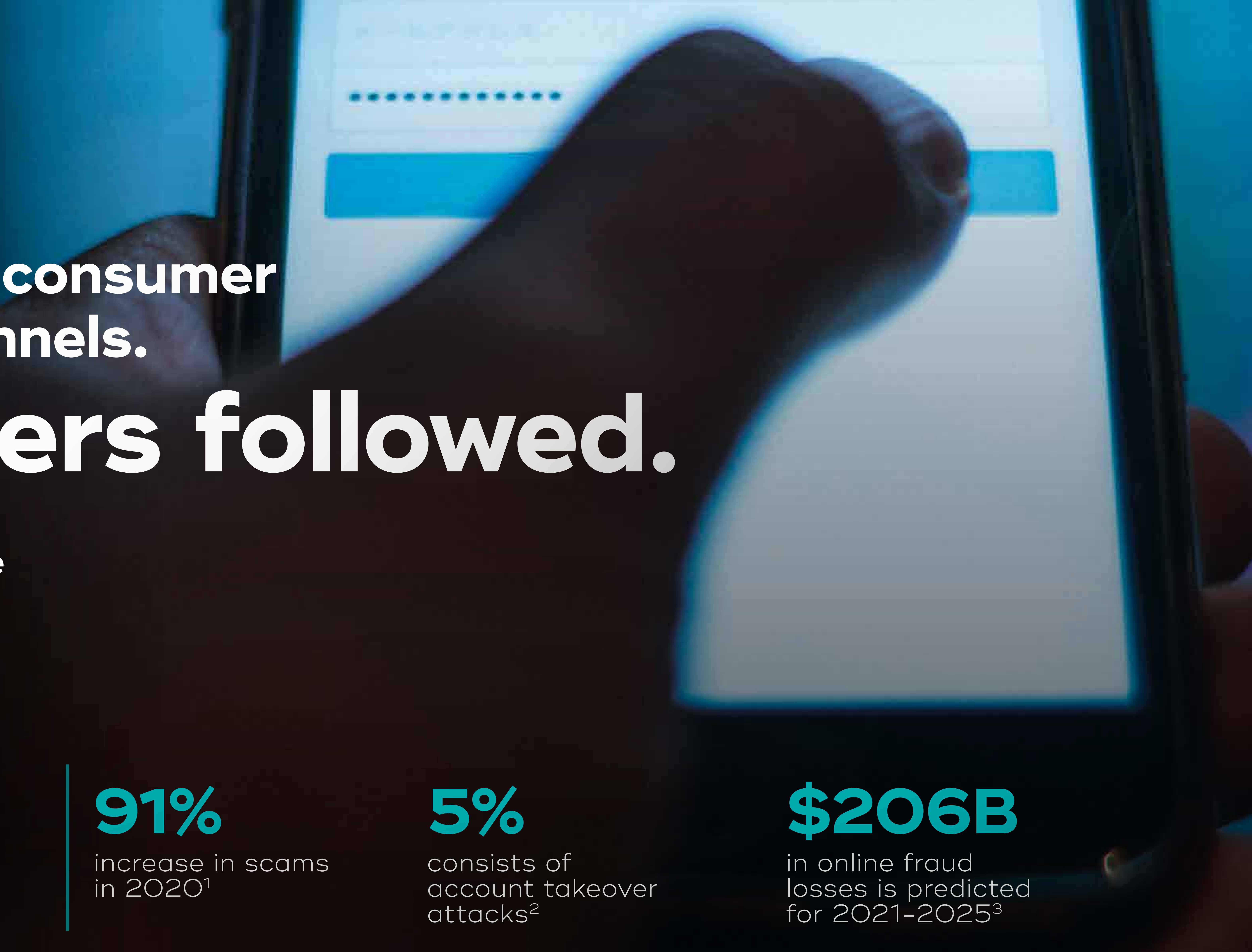
Digital fraud is skyrocketing. And it’s costing you.

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

celebrus

teradata.



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%

consists of account takeover attacks[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] Juniper Research, "Online Payment Fraud Losses to Exceed $206 Billion Over the Next Five Years; Driven by Identity Fraud"

Current solutions lack the sophistication to combat the rapidly evolving strategies fraudsters use to evade detection.

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

Fraudsters exploit weak links. Don't leave yourself vulnerable.

Vendors are rushing to add biometric support to their fraud solutions so they can claim their solution stops digital fraud. But these integrations have limited data collection and analytic capabilities. They check a box but don't have the processing power to prevent fraud.

You can't fight fraud when you don't own your data.

Most fraud solutions are closed-loop systems. Vendors collect and store biometric data in closed or anonymized cloud repositories where it can't be easily linked to customer transactional activity. But connecting all the data is where the power to fight fraud begins. That's why you need to own your data.

Fraudsters move fast. You need to move faster.

Data scientists must continuously create new models to battle the constant onslaught of novel fraud techniques. And traditional fraud solutions can't capture, store, and process the amount of detailed data needed to build and fuel these models.

The answer isn’t more data. It’s more data in context.

When it comes to detecting and preventing fraud, context matters. And so does speed.

Organizations need to be able to activate all relevant data in real time—including transactional and behavioral. A future-forward fraud solution requires five key capabilities:

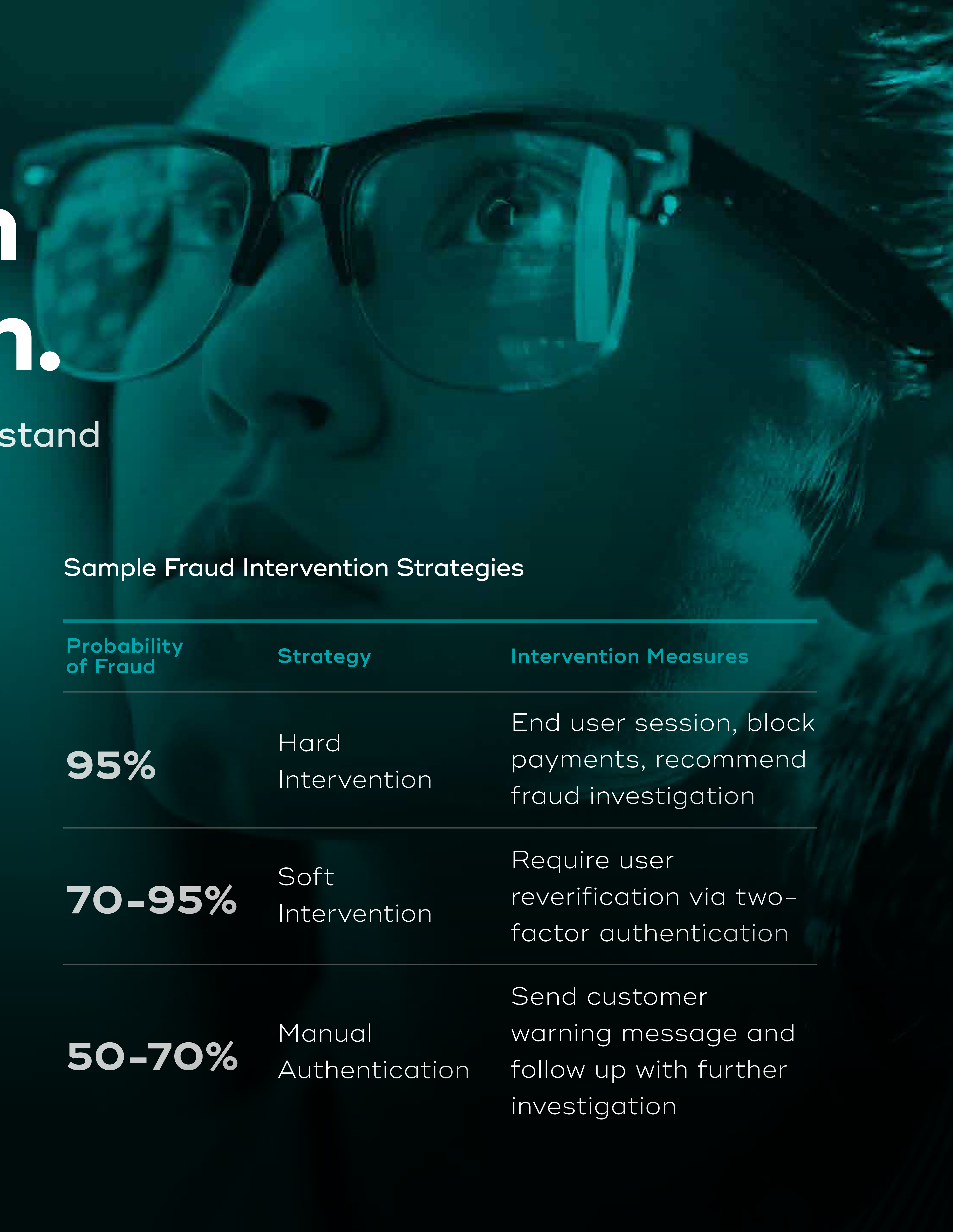
Combine transactions and interactions: Bringing together traditional transactional information with new data that describes digital interactions can provide contextual intelligence that allows for richer insights, including detection of fraud behaviors.

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 (AI) or machine learning (ML) model for every customer makes it possible to more accurately detect if interactions are genuine—or generated by bad actors.

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

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



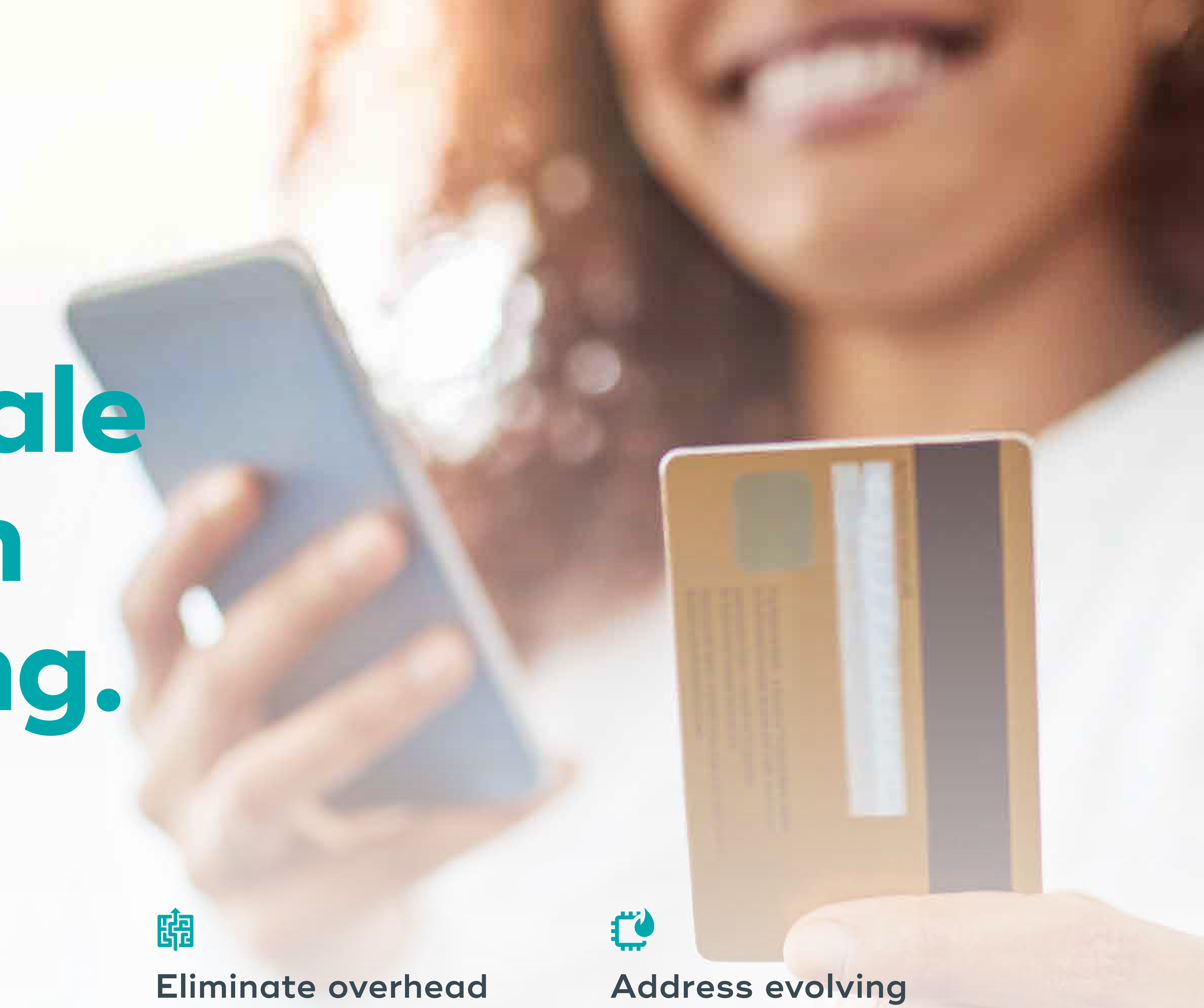
It’s time to switch from detection to prevention.

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

- **Watch** 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 using hyper-personalized AI and ML models to profile bad actors and genuine users, then use that data to allow legitimate activity and block fraudsters—all in real time.
- **Decide** if an intervention is required, and if so, determine the appropriate strategy, 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.

Sample Fraud Intervention Strategies

Probability of Fraud	Strategy	Intervention Measures
95%	Hard Intervention	End user session, block payments, recommend fraud investigation
70-95%	Soft Intervention	Require user reverification via two-factor authentication
50-70%	Manual Authentication	Send customer warning message and follow up with 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 stopping only fraudulent transactions, not legitimate ones

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

Eliminate overhead and improve efficiency by reducing fraud investigations, streamlining case management, and 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 increase 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% of fraud cases 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 Customer Experience Data Model within Teradata Vantage captures and organizes data from Celebrus in near real time.

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

The real-time capabilities of 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.

Teradata is the connected multi-cloud data platform 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**

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**

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