FRAUD PREVENTION / DATASHEET

Move from detection to prevention and outsmart tech-savvy fraudsters

Digital fraud—and the cost and complexity of managing it—is skyrocketing. As consumers move toward more interactions on digital and mobile channels, fraudsters have quickly developed new strategies to exploit those channels. With the emergence of real-time payments, losses happen fast and the ability to recover those losses is low.

COVID-19 further accelerated consumer adoption of digital channels—and fraudsters followed close behind. Customers expect seamless, protected experiences that keep pace with their fast-evolving digital behaviors. Escalating costs demand that fraud losses and the costs of fraud management be brought under control. And regulators are increasing pressure on banks to act fast. These factors have pushed fraud detection and prevention to the forefront, making it a top priority for the financial services industry.

If enterprises are to outsmart tech-savvy fraudsters, prevent losses, and deliver excellent customer experiences, they must tackle digital fraud by being able to:

- **Listen** by building a contextual view of each transaction
- **Understand** the fraud risk signaled by the customer behavior
- **Decide** if an intervention is needed and if so, how severe
- **Act** by delivering the intervention or transaction approval in real time

Challenges with current fraud solutions

Despite the growing impact and costs of fraudulent activity, current solutions for combatting fraud are inadequate. Both traditional and newer fraud solutions lack the sophistication needed to keep up with the rapidly evolving strategies that fraudsters are using to evade detection.

- **Traditional fraud solutions are transactional and backward focused, focusing only on transactions and 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.** They offer behavioral biometric analysis, but don't incorporate transactional knowledge. These solutions are low in precision and accuracy and typically lack explainability, which is a regulatory requirement in many jurisdictions.
- **Both new and traditional solutions are reactive, not preventative.** The majority of fraud solutions provide capabilities to detect and investigate fraud after it has happened but are unable to prevent fraud in real time.

Digital Fraud Landscape At-A-Glance

The number of scams grew
91% in **2020**[1]

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

$206 billion
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"

celebrus FRAUD DATA PLATFORM teradata.

To proactively fight tech-savvy fraudsters, organizations must leave behind reactionary, detection-centric fraud solutions that provide a limited view of transactions and behaviors. The future of fraud management is in contextually driven, prevention-centric solutions where decisions can be made in milliseconds.

Activating fraud prevention in four steps

To stop fraud, organizations must be able to:

1. **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.
2. **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.
3. **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.
4. **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

Switching from detection to prevention with data in context

Context matters for detecting and preventing fraud. Analysis of a customer's transactions or behavioral biometrics can't be performed in isolation. To quickly detect and prevent fraud, organizations must understand the environment in which the transactions are being made. This includes where the customer is, when they are active, how they interact, what they see, and the device they're using, all while considering historical and current transactional data.

That's why more data isn't enough to proactively fight fraud. To stop fraud before it happens, organizations need a solution that enables them to activate all relevant data in real time—including transactional and behavioral—to better detect and prevent fraud.

A future-forward fraud solution requires 5 key capabilities.

1. **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.
2. **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.
3. **Enable hyper-personalization with millions of models:** Training and deploying a personalized AI or machine learning model for every customer makes it possible to more accurately detect if interactions are genuine—or generated by a bad actor.
4. **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.
5. **Continuously learn and evolve:** Leveraging artificial intelligence (AI) and machine learning methods to continuously train on user behaviors provides the ability to detect new types of fraud tactics as they emerge.

Celebrus and Teradata enable fraud prevention at scale

There's a new way of fighting fraud that moves past the limitations of current detection-centric fraud solutions. Celebrus and Teradata have created a solution that enables organizations to understand bad actors and intervene in their journeys with preventative action in real time—or recognize and allow genuine transactions to proceed, enabling seamless and safe customer experiences.

With Celebrus and Teradata, organizations 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

This first-party method of data collection requires no tag management or complicated data layers. It uses a single line of code to capture all interactions from digital channels and pushes this data to Teradata Vantage™ to a pre-built fraud prevention data model. There's no work required to get a copy of the data as it's created and stored as an enterprise asset for the brand, ready to deliver multiple outcomes across many use cases.

All data collection, processing, and delivery to support decisions happens in real time—shaping a fast fraud intervention response and optimal customer experience. Connectors and APIs also allow subsets of the data to be sent where needed to drive interventions or approvals in a secure and compliant manner.

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. There were over 2,000 fraud cases per month and a loss of approximately $2,700 per case.

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.

SOLUTION

After deploying Celebrus and Teradata Vantage, 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

Results included:

250,000
Unique customer journeys an hour at peak times

70%
Cases of fraud are now detectable and preventable

$100 million
In preventable fraud detected

Unlock the full potential of fraud prevention with Celebrus and Teradata

Year after year, industry experts recognize Teradata as the cloud leader with our connected multi-cloud data platform for enterprise analytics. Teradata has partnered with Celebrus to enable organizations to prevent fraud at scale and in real time.

- 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.

Digital fraud is continuously evolving. With Celebrus and Teradata, organizations can finally stay several steps ahead of tech-savvy fraudsters, reduce fraud losses, and cut the cost of managing fraud—while also improving the customer experience.

About Celebrus

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**.

About Teradata

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. The Teradata Vantage architecture is cloud native, delivered as-a-service, and built on an open ecosystem. These design features make Vantage the ideal platform to optimize price performance in a multi–cloud environment.
Learn more at **Teradata.com.**

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

celebrus FRAUD DATA PLATFORM

teradata.