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 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. The cost of fraud management and fraud losses continue to escalate and must 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 be able to:

- **Watch** 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. These solutions lack the sophistication needed to keep up with the rapidly evolving strategies that fraudsters are using to evade detection.

- **Current fraud solutions have limited biometric capabilities.** 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.
- **Most fraud solutions are closed-loop systems—you don't own your data.** Instead, 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.
- **Current fraud solutions don't move fast enough.** Fraud can't be stopped with a single model; it takes thousands of models. Data scientists must continuously create new models to battle the constant onslaught of novel fraud techniques. But traditional fraud solutions don't have the ability to capture, store, and process the amount of detailed data needed to build and fuel these models.

The digital fraud landscape at a glance

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

5% of all digital traffic consists of account takeover attacks [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 Juniper Research, "Online Payment Fraud Losses to Exceed $206 Billion Over the Next Five Years; Driven by Identity Fraud"

celebrus | 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. **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.
2. **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.
3. **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.
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%	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

Switching from detection to prevention with data in context

When it comes to stopping fraud, context matters. Analysis of a customer's transactions or behavioral biometrics can't be performed in isolation. To quickly detect and prevent fraud, organizations must understand 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 five 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 (ML) model for every customer makes it possible to more accurately detect if interactions are genuine—or generated by bad actors.
4. **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.
5. **Continuously learn and evolve.** Leveraging artificial intelligence (AI) and machine learning (ML) methods to continuously train on user behaviors provides the ability to detect new types of fraud tactics as they emerge.

Teradata and Celebrus enable fraud prevention at scale

There's a new way of fighting fraud that moves past the limitations of current detection-centric fraud solutions. Teradata and Celebrus have created a solution that enables organizations to profile both genuine customers and bad actors. Legitimate activity is recognized and allowed to proceed—enabling seamless and safe customer experiences—while fraudsters are blocked in real time.

With Teradata Vantage™ and Celebrus, organizations 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

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 Vantage to a pre-built Customer Service Data Model. Data scientists and analysts can then build sophisticated fraud prevention models using Vantage's advanced analytic capabilities and third-party analytic tools and languages.

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 future losses.

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 with sub-second response times

Results included:

250,000
unique customer journeys per hour at peak times

70%
of fraud cases are now detectable and preventable

$100 million
in preventable fraud detected

celebrus | teradata.

Unlock the full potential of fraud prevention with Teradata and Celebrus

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 Customer Experience Data Model within 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.

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

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.**

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**.

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