



CUSTOMER INTER@CTION *Solutions*®

Call Center Technology

Changing Times, Changing Data Management

The artery of contact centers is real-time data: customer identifiers, interactions, transactions, and responses that live agents and increasingly automated voice, e-mail and Web applications capture and transmit. With the need to learn more about customers, and to meet their needs more effectively comes the need to handle more data. How that data is managed: including accuracy, handling and processing is key to organizations' success. That includes ensuring data security and privacy backed by a growing array of laws.

We approached leading enterprises representing a wide range of data solutions with questions about real-time data management including on:

- Any potential data handling and bandwidth issues, including for at home agents
- Energy consumption and environmental footprint
- Data security and privacy
- Data accuracy

Here is a selection of their responses:

LiveOps (www.liveops.com)
Paul Lang, Senior Vice President, Product Management

We feel that real-time data handling within contact centers is for the most

part well-in hand. For home agents bandwidth needs to be factored in. There needs to be broadband connection and a dedicated telephone line to ensure quality service.

Privacy and data security are becoming paramount and applications should be explicitly configured to exclude logging of sensitive information such as social security numbers or non-public personal information data. There is the ongoing need to regularly audit systems and data for compliance.

There are a number of standards that have been set as security benchmarks. These include PCI-DSS (Payment Card Industry Data Security Standard), Health Insurance Portability and Accountability Act and ISO 27001 and 27002.

Oracle (www.oracle.com) Rich Caballero, Vice President, Service Products

The applications must be tuned and optimized to receive large amounts of data in real time. If not, the user experience degrades significantly as user-interface response times increase and the data is not refreshed in a timely manner. Properly engineered solutions will also reduce the network bandwidth and processing power required. Service organizations should make sure that their on demand or on-premises applications can scale to meet their needs.

Oracle uses advanced database technology, server virtualization, and query optimization to minimize network bandwidth and CPU utilization. This in turn reduces the power and cooling requirements. In addition, the Oracle data center facility itself has been designed from the ground up to optimize consumption and footprint.

Many of our customers are taking three steps to reduce fraud and enforce data security. The first is around authentication. A customer must positively and uniquely identify himself in order to interact with a contact center agent. To make this

process as simple as possible, self service IVR or voice biometrics are being adopted.

Second, all sensitive data must be destroyed or encrypted. Any organization processing credit cards must be PCI-compliant which requires the agent to be able to erase any credit card information from a recorded conversation. If there is credit card information in a chat or e-mail transcript, then that information must be encrypted and transferred using secure FTP.

Finally, proactive alerts to detect fraud are being deployed. Predictive analytics can be leveraged to alert contact center agents in real time to identify potentially fraudulent activity and prevent it from happening.

With more personal information available online, privacy is certainly a growing concern. The best practice is to give customers control and monitor any agent access activity, making it very easy for them to change contact preferences online. This allows customers to control how a business can use their personal contact information.

The application should prevent service agents from having visibility to any personal information without first getting explicit permission from the customer. This permission should be recorded either via a voice recording or chat/e-mail transcript.

Finally, any agent activity must be recorded and stored. Every action that an agent takes within the application should be auditable. Any chat or remote control sessions should be recorded and attached to the customer record.

Data quality is one of the biggest challenges organizations face. The value of your CRM application is directly proportional to the accuracy of the information in it. The explosion

of contact information has simply increased this challenge.

Step one is to create a customer master that is the single source of truth with respect to contact details and preferred communications channel. Step two is to ensure that if contact details are to be edited or new contact records created, the master must first be consulted and any resulting conflicts raised and resolved in real time. Finally, it is important that customers can update personal profiles online and those updates are immediately reflected in the customer master.

**Teradata (www.teradata.com)
Dr. David Schrader, Director of
Strategy and Marketing**

As technology improves, an increasing percentage of customer interactions can be handled by the Web or IVR systems, with contact center agents handling dialogues that cannot be automated. Volumes on all these systems are going up, driven primarily by customer convenience.

The data input and output volumes and rates from contact centers can be sizeable. Uploading data from the contact center to the data warehouse may require parallel loads to keep up with volumes and short latency time goals. Most contact centers use portlets that use service oriented architecture callouts to obtain next best offer recommendations from the data warehouses to paint the agents' screens. So far, Teradata customers have experienced no problem with the capacity, either in data record sizes or latencies for inputs or callouts, which usually require sub-second response times.

We take energy consumption concerns seriously. For example, our latest 5550 series Active Enterprise Data Warehouse Server uses approximately 75 percent less energy and coexists with multiple generations of Teradata servers, thereby protecting customers'

technology investments. The 75 percent reduction in electricity usage for the same capability data warehouse, as compared to Teradata servers of three to five years ago, is enough kilowatt-hours saved by one typical system to power 40 U.S. homes for one year. In addition, the 5550 Server reduces the floor space requirement by approximately 66 percent. By dramatically reducing energy usage for the same system performance, Teradata has also reduced associated data center cooling and power delivery infrastructure costs by a similar ratio.

Good data security depends on more than just contact center data handling, but requires a much more holistic approach. Using an integrated, enterprise data warehouse, accompanied with data governance best practices, is a viable and lower-cost approach to provable compliance and audit-ability than handling data security using a touchpoint by touchpoint piecemeal approach.

At the heart of any privacy program is respect for the customer, transparency in information collection and use, and--at the bottom line--returning value to the customer in return for information. Teradata's customers have learned over the years that when information is used to help or even "delight" customers by correctly anticipating their needs, the privacy issues diminish. It's all about fair use. Again, it's wise to tighten database security practices, taking strong measures such as those we mentioned above. These will help ensure data privacy.

**TARGUSinfo (www.targusinfo.com) Paul McConville, Executive
Director**

More contact centers are working with external partners to analyze, understand, host and make data actionable. This allows contact centers to focus on their core competencies. It is critical, though that this data can be accessed and leveraged in real time.

At TARGUSinfo, our infrastructure was built from the ground up to handle tremendous loads of data. Per year, we handle more than 50 billion interactions across our network-- something that sets us apart.

We have not seen technology limitations with our contact center partners that deploy at home agents. It is critical, though, that at home agents work on a system that is tied to

a central system that can incorporate and deliver customer data and scores.

Regarding data security I have three suggestions:

1. Only take data that is absolutely necessary.
2. Limit access to customer data only to those that MUST access it to perform a clients' request.

3. Do not allow client data to be stored or copied to any device that can travel outside a secured facility.

Data privacy is definitely an issue for many industries, such as financial services and health care. Consumers trust that their personal information will be used only to the extent that they allow, such as to typically only fulfill transactions.

How Beryl Handles Real Time Data

To get an idea of some data-handling and privacy issues faced by contact centers, The Beryl Companies, a teleservices firm specializing in serving healthcare organizations with inbound and outbound contact management offers an excellent example. Its 194-agent "call advisor" contact center at its Bedford, Texas head office handles sensitive data in real-time and near-real time. Information that is subject to stringent privacy laws like HIPAA.

Beryl has traditionally taken primarily inbound calls from healthcare consumers seeking information about physicians and classes available at their local hospitals. It has been asked by clients to provide increased and data-intensive services. For example it has been making more outbound calls for appointment scheduling and reminders, Web site-originated call-me-back-requests, and post discharging calling services, reports CIO Jim Stalder. That has led to a growth in real-time/near-real time data. In response Beryl is now offering new products that make the exchange of data between it and its clients more real-time in nature as compared with periodic updates such as physicians' contact information.

"For example, with our post discharge calling services, we need information from our clients on a daily basis about which patients were discharged from the hospital," says Stalder. "When we make those calls, we may also need real-time access to a particular patient's discharge instructions."

The real/near-real time data environment at Beryl has made error and exception handling increasingly important. In the past, when data was infrequently updated, such as physicians' contact info, it was acceptable to realize a day or two after the data has been received that there may have been problems with the formatting or contents of the received file. However, when the contact center products are near real-time, it is important to know in real-time if and when there is an error in that data.

"Otherwise, you might end up calling a patient to remind them of their appointment after their appointment was supposed to have taken place," says Stalder. "Or, you might have your contact center agents waiting around to start making calls, thereby losing time and productivity if there were problems with the data load and you didn't realize it until after the shift started."

Beryl has been carefully and imaginatively managing privacy issues. The written contracts between Beryl and its clients establish Beryl as a business associate and provide protection and limitations on using protected (personal) health information (PHI). All Beryl employees also receive HIPAA training as a standard part of their training and sign confidentiality statements upon completion.

To ensure privacy as well as to limit the amount of data handled Beryl has been working with its clients to minimize the amount of PHI that resides in its systems. In one particular case, Beryl's agents use a secured network connection to access one of its client's electronic medical records systems. They have unique user IDs and passwords into the client's system; the clients control what aspects of the medical record a Beryl advisor can access.

"A side benefit of this approach is that our clients can then audit and log all access by Beryl to their medical records," reports Stalder. "This is a significantly more secure and private approach to managing the data compared with Beryl getting a copy of the data and needing to take all the precautions around securing the data and auditing usage."

If this trust is breached, there can be significant consumer backlash. Businesses must be sure to have a detailed privacy policy and should disclose any data uses to customers. It should be easy for customers to control data uses, choose communication preferences and opt-out if they wish their data to be destroyed/removed.

The rise of wireless and VoIP calls have impacted list accuracy as they account for over 50 percent of inbound calls to most contact centers. It is now tougher to instantly identify the names, addresses and previous purchases at the moment of interaction because phone numbers, previously a reliable identifier, are far more fluid. It is easier for people to change phone numbers, have multiple phone numbers and have phone numbers that are not tied to a precise geography.

It is critical for phone-centric companies to work with phone-centric data providers that are updating their customer records (i.e. linkages of name, address and phone number daily.) They should be sure to ask their data partners about their coverage of cellular and VoIP data. They should also be sure to understand how their data partner is supplementing phone data with other sources to ensure broad household coverage across the U.S., which is critical for real-time scoring. **CIS**