



**A Public Agency**

# COLLECTION AND RECYCLING PROGRAM SUPPORT AND COMPLIANCE



---

**Agenda Item 6A**

**Presentation by Recology Summary of Impacts of the November 2023  
Cyber Security Incident**

**No Staff Report Attachments Only and Presentation by Recology**

---

**Attachments:**

- A. Letter from Recology detailing Impacts of the November 2023 Cyber Security Incident



**SENT VIA EMAIL**

June 14, 2024

Joe La Mariana  
Executive Director  
RehinkWaste  
610 Elm St, Suite 202  
San Carlos, CA94070

**Re: Summary of Recology's Cybersecurity Incident**

Dear South Bayside Waste Management Authority (SBWMA) Board of Directors,

Per your email dated May 7, 2024, this correspondence is intended to provide a summary of events and impacts of the cybersecurity incident suffered by Recology San Mateo County (collectively, "Recology"), and to respond to specific questions asked about the incident.

Recology experienced a cybersecurity incident on November 2, 2023 that affected some of Recology's systems and applications. Recology is just one of several organizations nationwide whose information technology systems were impacted by similar incidents. Information about these incidents were documented by several media outlets and initial information shared at the SBWMA Board Meeting on November 16, 2023 following the incident.

**System Impacts**

As you are aware, the November 2, 2023 cybersecurity incident affected the ability of Recology personnel to access several systems and applications that support our day-to-day business activities. Certain applications and data files typically accessed through the Company's network platform were rendered unavailable to Recology personnel for several days or weeks, depending on the application and type of file.

These accessibility issues affected our ability to interact with certain applications and data, including systems that maintain routing and route data, customer collection frequency, cart size, and subscription data, scale data and tonnage information, files and reports stored on 'share' drives, and historical data used to produce monthly, quarterly, and annual reports. Despite these access issues, we relied on backup processes where possible to record and report data manually. These processes are described in more detail below.

Shortly after the incident, third party cybersecurity experts were retained to provide forensic analysis and restoration assistance. These experts determined that data contained within Recology's customer and financial databases were not compromised. However, the network platform used to access certain systems, applications, and data was affected by the incident. Recology's information technology team, in conjunction with outside cybersecurity experts, began restoration of the company's network platform, in addition to bolstering the company's cybersecurity endpoint detection and response and device authentication protocols. During the initial restoration efforts, select critical system users from Recology's finance and operations teams were temporarily relocated to Vacaville to enable these users to access the system within a protected environment to perform critical functions.

In late November 2023, remote access was restored for select users. Access was expanded to a larger group in December. As restoration continued in the coming weeks, additional users were provided system and application access. By mid-January, our systems were ready for restored access by all users.

Recology's operating systems and applications are now back online, and Recology users have regained system and application access. As discussed in greater detail below, the Routeware system for Recology San Mateo County was brought back online in May with updated tablets.

### **Routing**

Our ability to use Routeware, our third-party routing and route information system, was affected by the cybersecurity incident. Digital real-time route data and communication between our dispatch system and trucks on route could not occur through the Routeware system. In addition, real-time route modifications and drivers on route recording data into the system in real-time could not occur. However, like our other systems, manual backup processes were put in place to ensure route information and data was recorded and any necessary information could be exchanged with drivers while on route.

Recology maintains a hard copy library of route maps, route manifests, and other routing information that can be provided to drivers. This information provides drivers with the information they need to perform regular collection service. Other real-time information that would normally be communicated through the Routeware system is communicated directly to drivers on route via company provided cell phones. Drivers on route can manually record necessary route information on handwritten logs that are submitted to the dispatch office and then manually entered in the system at the end of the day.

Although our back-office functions are not as efficient as our Routeware system, by large, regular service to customers were not affected by the disruption to this system.

### **Collection Service**

Despite the system issues, Recology crews continued performing collection services without interruption or disruption to our customers. Recycle, Compost, and Garbage containers were

collected on their regularly scheduled days within normal collection times. In addition, our customer service staff continued to answer phones, take customer calls, and respond to customer emails. Our facilities and offices remained open and accessible to our employees and the public during our regular business hours. From a collection service perspective, the system issues were largely unnoticed by customers.

### **Customer Service**

Although it was seemingly business as usual for customers from a service delivery and collection perspective, there were some impacts on the customer service side.

Instead of being able to access customer account information instantaneously and process customer requests in real time, as is typically the case, Recology's customer service representatives were forced to take manual notes of a customer's request and at times, inform the customer that they would process the request and get back to them in the coming days. Communication between our customer service team and our operations and finance teams—for example, to obtain information or to process changes in service— had to be done by, shared spreadsheets, email, or by phone, instead of happening automatically through our customer relationship management (CRM) system. Upon regaining access, all customer requests that required manual tracking have since been updated in our CRM system, to maintain an accurate history of customer requests.

### **Billing**

Delays in customer bills were also experienced during this period. Residential customers would normally receive their bills by the 29<sup>th</sup> of November, however, bills for this billing group did not get released until December 5<sup>th</sup>. Commercial and multi-family customers billed monthly would normally receive their bills by the 29<sup>th</sup> of the month, but during November and December, these customers experienced a four (4) day delay in receiving them. Now that we are largely through this cybersecurity incident, these billing delays have been corrected and we are back to our normal billing schedule.

### **Personal Information**

In addition to restoring impacted systems, Recology has been working with forensic experts to determine whether any personal information was accessed or acquired during the incident. This work is ongoing. While Recology is not aware of anyone's information having been misused, the review did identify evidence of some personal information having been acquired without authorization. Notifications have been sent to those individuals. Most of the affected individuals who received notice are our employees, former employees, prospective employees, or the beneficiaries or dependents of employees. Recology also provided notice of the incident to the Office of the California Attorney General.

## **Reporting**

As we have discussed in our various conversations and through this correspondence, a number of Recology's systems and applications were impacted by the cybersecurity incident. These included the systems that manage and maintain some of the transactional information and data that is used to produce the monthly, quarterly, and annual reports that are distributed to the SBWMA. To assure security, global access to this information has been brought back online slowly and carefully. Data entry of manual transactions started to occur in the weeks following the incident and has since been completed.

As a result of the incident, the data used to produce and create our regular financial and operational reports has not been as readily accessible or available to all staff members as it would have been under normal circumstances. As a result, some of the financial and operational reports that we produce and distribute on a regular cadence have been delayed.

Delays were communicated to SBWMA Staff and other stakeholders that our regular deadlines for these reports could not be met. We greatly appreciate your patience and understanding while we continue to work through our cybersecurity incident.

## **Improving Security**

Recology has gone to great lengths to safely recover from this cybersecurity incident. Part of our system recovery plan includes a component of rebuilding affected systems. These rebuilt systems are expected to be more durable and better fortified against future cybersecurity incidents. Our information technology team has also taken steps to further strengthen system security and is exploring whether additional steps may be warranted. We are confident that we will emerge from this incident with a system that is better able to avoid future disruptions and maintain business continuity.

## **Summary**

Recology suffered from a cybersecurity incident in November 2023. This incident affected various systems and applications that support Recology's day-to-day business operations. Despite the impacts of this incident, there were minimal service delays and/or disruptions to customers. Customer phone calls continued to be answered and customer emails continued to be responded to during this time. Recology's offices and facilities remained open to the public and operational during regular business hours. Minimal customer service department and billing delays occurred for a temporary period of time.

All Recology's systems have been restored and are now back online. Going forward, Recology expects to have an information system that is more durable and better fortified against cybersecurity incidents in the future.

Again, we greatly appreciate your patience and understanding as we continue to work through this cybersecurity incident. We sincerely value our partnership with the SBWMA and these past few months have shown us that you value this partnership as well! If you have any questions or would like to discuss this information in more detail, please feel free to contact me.

Kind Regards,

A handwritten signature in black ink, appearing to read 'John Zirelli', written over the printed name.

John Zirelli  
General Manager  
Recology San Mateo County