Complete Update

TD Bank, the 10th largest bank in the US, confirmed this week that a former employee had unauthorized access to and shared sensitive customer data from August to December 2022.

This story is making headlines in 2025, seemingly because of a $5 million class action lawsuit currently underway. While the breach occurred in 2022, it serves as an important reminder for banks to properly conduct employee exit processes, audit user access for all applications, and put proper controls in place for all applications, especially for cloud-based applications. **TD Bank Confirms Data Breach: Account Numbers and Sensitive Customer Info Exposed - Benzinga**

CCI recommends banks risk-rate all their remotely accessible, cloud-based applications. On a quarterly basis, for those highest-risk applications, banks should ensure that access is appropriate, that all terminated employees have had their access removed, and that proper controls, such as IP restrictions and MFA, are in place.

Allowing a disgruntled ex-employee to, after termination, for example, access a cloud-based system with customer information could be costly for the bank money, as evidenced by the current 5-million-dollar lawsuit against TD Bank. It could also cost the bank significant reputational damage by having to send out a letter like the one TD did, as shown **here**.

David McPhillips

Complete Compliance, Inc. | Email | Website | Newsletter | IT Newsletter |(402) 939-6715