Legal Options When Bank Employees Take Confidential Data from Bank Systems

Anton Janik, Jr.
ajanik@mwlaw.com
(501) 688.8888

Lizzi Esparza
eesparza@mwlaw.com
(479) 464.5660

01/08/2024

Despite bank policies, training, computer warning banners, governing laws and banking regulations, bank employees still take bank or customer data as their employment ends. They take potential or current customer lists, transactional data and supporting customer files, procedural manuals, or other confidential or proprietary information including data protected here in Arkansas by the Personal Information Protection Act or federally by the Gramm-Leach-Bliley Act and its ensuing regulation. Here are ways to manage data theft by bank employees.

Policies should be set in place. Employee access to data should be limited to only that data needed to perform daily duties, and controls should be put into place to monitor and protect against credential sharing and inappropriate access to data. Make sure your policy forbids the removal of confidential data, including personal financial information and state protected information, from bank systems to personal devices or personal email addresses. Consider the use of formal confidentiality and nondisclosure agreements.

Actively monitor and keep logs of network, device and computer activity. Consider preserving an image of the former employee's company hard drive, or at least their complete email account, when that employee leaves. Your infosec or internal audit team can easily catch the transmission of data to external email addresses. Have software and systems in place to catch the move of data to personal devices, like USB drives.

If data theft is found, engage your legal team to help determine the scope of the loss. This includes whether the data contains any confidential information or that protected by state or federal law. For current and prospective customer lists, explore actual and likely damage from that loss. Keep in mind that your internal procedural manuals have value to your competitors, especially smaller competitors including smaller loan operations.

In most cases, your legal team will notify the former employee in writing regarding the theft. The letter should provide enough information about the loss to show the employee that they have been caught, remind them of the bank policies, demand that they permanently delete any bank data they possess, and that they detail whether they have transferred or shared that data with anyone else. Where state or federally-protected data is involved, remind them of mandated breach notification laws. You can provide that costs for same will be charged back to the employee. Also send the employee an affidavit which confirms the removal and ensuing deletion of that data and all copies, that it was not further transmitted, and that addresses the employee's job, scope, tenure, and recognition of governing bank policy and procedure. For further proof of deletion, you may require access to the account or device.

Send a letter to the employee's new employer. Alert the new employer to the theft, identifying the data by title or subject matter, and asking them to confirm that the data has not and will not be uploaded into their systems.

Further options. If the former employee won't cooperate with this process, further options are available. Under section 38(k) of the Form 101/Suspicious Activity Report, banks are under an obligation to report the misuse of position or self-dealing to FinCEN. Include information on the policies and procedures in place, the dates and scope of the theft, the depositor prejudice, the financial impact to the bank and depositors, and the employee's disregard with your attempts to resolve this. The Federal Reserve can issue an Order of Prohibition barring the employee from participating further in any banking activity.

Finally, you may also sue the former employee for damages arising from that theft of customer data, bank confidential documents and strategic materials, and the costs of mandated notification.

Anton Janik CIPP/US, CIPP/E and Lizzi Esparza CIPP/US are information privacy, security and data rights attorneys.