STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL
120 BROADWAY
NEW YORK, NY 10271

ERIC T. SCHNEIDERMAN
ATTORNEY GENERAL

(212) 416-8050

June 5, 2015

Mr. Stephen M. Cutler
General Counsel
JP Morgan Chase
270 Park Avenue
New York, New York 10017

Dear Mr. Cutler:

I write as part of my Office's ongoing effort to help banks upgrade their security protocols to protect the personal identities and financial well-being of customers from unscrupulous employees.

During a multi-year investigation into identity theft schemes perpetrated with the assistance of bank tellers, my Criminal Enforcement and Financial Crimes Bureau exposed tellers at some of New York's largest banking institutions who stole millions of dollars from hundreds of bank customers residing throughout New York State and in other states on the East Coast.

"Operation Pen & Teller" revealed common security weaknesses in the banking industry that allowed these schemes to go largely undetected. These vulnerabilities allowed bank tellers at local branches to easily obtain the personal identification information of account holders across multiple states, while making it difficult for bank supervisors to identify this fraud.

For instance, tellers frequently retrieved customer account numbers and Social Security numbers from bank databases, without authorization or a legitimate business need. Tellers sometimes provided this stolen information to co-conspirators, who used it to create fraudulent identification and financial documents. These fraudulent documents were then used to impersonate account holders, to circumvent bank security procedures, and to withdraw money directly at bank branches or through the use of fraudulently obtained debit cards.

Even though the perpetrators of these schemes have been arrested, and several are already serving time in prison, bank customers are still at risk. I have attached a document that describes several common weaknesses we encountered in our investigation, and that proposes reforms to better protect bank customers. We believe these measures can be implemented relatively easily, and, if your institution has not already addressed them, I urge you to do so without undue delay.

We look forward to discussing these proposals so that together we may better safeguard New Yorkers and our financial system. Please contact Gary T. Fishman, Chief of my Criminal Enforcement and Financial Crimes Bureau, at (212) 416-8926 if you have any questions or wish to discuss the proposed reforms.

Sincerely,

Eric T. Schneiderman

Identified Bank Vulnerabilities and Proposed Compliance Reforms

1. Vulnerability: Scope of Access by Employees. The schemes we investigated were predicated on the ability of newly hired tellers to exploit their unfettered access to all customer data, including full account transaction histories, balances, social security numbers, and other personal identifying information belonging to account holders across the country. Our investigation revealed that after a brief training period, newly hired tellers were usually provided with unlimited access to financial institution ("FI") customers' account data. Tellers were also permitted access to accounts without customers present and could view any type of customer data. Furthermore, access was not limited to either the geographic location of the teller's branch or the account holder's domicile.

   Proposed Reform: FIs should develop protocols to ensure that bank tellers and other employees are permitted to access personal identifying information only when there is a legitimate business purpose for viewing such data. There should be limited access to databases based on each employee's position and their need for this data. For example, FIs should limit employee access to only those customer accounts in the immediate geographic region of their local branch, unless given specific approval by a supervisor. In addition, there should be limitations on the type of customer account information that an employee can obtain without a live customer counter transaction or prior supervisory approval.

2. Vulnerability: Lack of Regular Employee Audits. Our investigation revealed that branch supervisors typically do not have reasonable and regular access to an audit trail for account information accessed by a particular employee. If a supervisor had reviewed the volume and scope of customer accounts retrieved by the tellers, it would have been immediately apparent that numerous accounts had been accessed each day with no legitimate business purpose.

   Proposed Reform: Branch supervisors at FIs should have access to an automated daily report of accounts retrieved by bank tellers and other employees, and any corresponding transactions completed for such accounts. This will enable supervisors to regularly monitor employee access and to identify employees who retrieve account information without conducting a corresponding financial transaction, or from accounts outside of their immediate geographic region.

3. Vulnerability: Customer Call Centers. The schemes prosecuted by my office also exploited call center and automated bank telephone systems used by consumers to make account inquiries and check account balances. In some cases, after corrupt tellers obtained confidential information from a customer's account, other fraudsters called into these telephone systems and used the stolen customer data to make sure there were

sufficient funds in a particular account before attempting to make an unauthorized withdrawal. On many occasions, a single telephone number was used to obtain information for multiple unrelated accounts; however, this information was not transmitted across departments or silos at the FIs.

Proposed Reform: FIs should implement security systems for their call centers and automated bank telephone systems to track instances in which a single telephone number is used to seek information about unrelated accounts. Once detected, the security system should trigger an immediate fraud alert to the corresponding customer and temporarily freeze the accounts. FIs should also file a Suspicious Activity Report (SAR) when they identify a telephone number used to check multiple unrelated accounts.

4. Vulnerability: Resignation of Employees. Our investigation further revealed that on many occasions, after being initially questioned about questionable efforts to obtain confidential information, bank tellers resigned, and the FIs ended their investigation. These corrupt tellers then simply gained employment at another FI and resumed committing fraud.

   Proposed Reform: When an employee resigns in response to questioning, the FI should continue with its internal investigation, including conducting an audit of the employee's account access and corresponding transaction history, and file a SAR. In addition, when an employee resigns immediately after being questioned about abnormal activity, the FI should make this fact part of the employee's personnel record. FIs should also exercise enhanced due diligence when considering hiring a prospective employee who recently resigned from another FI.

5. Vulnerability: Lack of Robust Employee Monitoring. FIs already have robust Know Your Customer (KYC) policies and procedures. These procedures ensure that accounts continue to operate in the manner in which they were intended. KYC requires ongoing diligence from FIs. Our investigation revealed that FIs typically do not have in place a similar level of ongoing due diligence for their employees. In fact, we found a lack of policies and procedures designed to test whether employees continued to behave in the manner expected when they were hired.

   Proposed Reform: Similar to KYC policies and procedures, FIs should strive to establish and promulgate robust Know Your Employee (KYE) policies and procedures. If employees were monitored as part of a FIs ongoing compliance program, fraud would be more easily identified and customer data better protected.