



Enterprise Bank

December 29, 2014

Joseph Foster, Attorney General
New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Enterprise Bank Incident October 30, 2014

Dear Mr. Foster,

This letter is being sent to report an incident of unauthorized access to certain client information maintained in our Investment Advisory area of Enterprise Bank located at 222 Merrimack Street, Lowell, MA. This letter will outline the nature of the incident, the number of clients impacted, and the steps management has taken in response to the incident.

On October 31, 2014, we were notified by an existing client of our Investment Advisory department that when he accessed his account online in the Trust client portal on October 30, 2014, in addition to his own account, he was able to view the account number, account name, and market value of all of the clients of the Investment Advisory division of Enterprise Bank. Information for approximately 582 accounts, could be viewed. 63 of these accounts belonged to 41 New Hampshire residents.

Although the client was able to view the information, he was not able to modify client information or perform transactions on client's accounts. No Social Security Numbers, dates of birth, license numbers, PIN's, and/or client portal usernames or passwords were included in the information that was viewed. No information relating to Enterprise Bank's core system (loans and deposits) is accessible through this portal and could not be viewed during this unauthorized access.

Immediately following receipt of notification from the client, access to the Trust client portal for Enterprise Bank was disabled. We worked with our service providers to determine how the unauthorized access was granted. We were able to determine this one client accessed the portal for approximately 20 minutes. Once this client's access was removed and a review of all client portal access was verified, we were able to re-activate client access to the Trust client portal on November 3, 2014. As a result of this incident, the software providers; modified default access codes, increased audit logging of user and client activity, and enhanced management reporting of user access activity and settings.

We have spoken with the client who had access to the portal and he has stated that he did not intend to take, use, transmit or otherwise compromise the client personal information contained in the database report. He did not knowingly take any action that compromised the security, privacy, confidentiality or integrity of the client personal information contained in the database report. He has advised us he will not misuse, disseminate or disclose any client personal information contained in the database report. He has securely destroyed all hard copies and

electronic copies of the database report that he had in his possession, or he has delivered all copies and/or electronic files to personnel of Enterprise Bank. Aside from the instances described above, he (i) did not further download, transfer or copy, (ii) did not allow anyone else access to, and (iii) has not retained, in any format, any client personal information contained in the database report.

In addition to working on identifying and notifying all of the Investment Advisory clients that have been impacted, Enterprise Bank is in the process of notifying; the Massachusetts and New Hampshire Division of Banks, the Massachusetts, New Hampshire, Connecticut, New York and Vermont Attorney Generals, the Massachusetts Office of Consumer Affairs and Business Regulation, the New York Division of State Police, New York State Division of Consumer Protection, the Federal Reserve Bank of Boston, and the Federal Deposit Insurance Corporation.

A formal notification to all customers affected will be mailed on December 29, 2014. Enterprise Bank will also inform the three national consumer reporting agencies of the incident.

Customers will be provided with the following information and guidance:

- A recommendation that the customer review investment account statements and immediately report any suspicious activity to the Bank;
- A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports;
- A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and information relating to how to have fraudulent transaction deleted;
- An explanation of how the customer may obtain a credit report free of charge;
- Information about the FTC's online guidance regarding steps a consumer can take to protect against identity theft and the FTC address and toll free telephone number that can be used to obtain identity theft guidance and report suspected incidents of identity theft;
- A one year subscription to an Identity Theft product from Deluxe free of charge;

Management is in the process of reviewing and assessing procedures that will help prevent the occurrence of this type of unauthorized access in the future. Initial steps will include additional training for employees, and Investment Advisory procedures will be enhanced. Changes as a result of this incident will be reported to the Board's Enterprise Investment Advisory, Banking Technology Steering and Audit Committees.

