



comply with the Massachusetts Data Breach Law, G.L. c. 93H, and the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 C.M.R. 17.00, *et seq.*

4. The Bank denies that it has violated any Massachusetts laws or regulations in connection with the Incident, or that it engaged in any wrongdoing. Without admitting to the Attorney General's allegations or to any violation of law, the Bank has voluntarily and knowingly entered into this Assurance of Discontinuance in order to avoid the time, expense, and uncertainty of litigation. The Attorney General agrees to accept this Assurance of Discontinuance pursuant to G.L. c. 93A, § 5, in lieu of commencing an enforcement action pursuant to G.L. c. 93A, § 4.

## II. THE PARTIES

5. The plaintiff is the Commonwealth of Massachusetts, represented by the Attorney General.

6. Defendant, TD Bank N.A., is a national bank with headquarters in Portland, Maine and Cherry Hill, New Jersey.

## III. DEFINITIONS

7. For the purposes of this Assurance of Discontinuance, the following definitions shall apply:

- a. "Backup Tape" shall mean a magnetic tape data storage device that is designed to be portable and to store large volumes of digital information, such as copies of computer servers and network applications.
- b. "Breach of security" shall have the same meaning as defined in G.L. c. 93H.
- c. "Data Breach" shall mean a "Breach of security," the acquisition or use of

Personal Information by an unauthorized person, or the use of Personal Information for unauthorized purposes.

d. "Effective Date" shall mean the date of filing of this Assurance of Discontinuance.

e. "Notice" shall have the same meaning as defined in G.L. c. 93H.

f. "Personal Information" or "PI" shall have the same meaning as defined in G.L. c. 93H and 201 C.M.R. 17.02.

g. "Service Provider" shall have the same meaning as defined in 201 C.M.R. 17.02.

h. "Transportation Service Provider" shall mean a Service Provider the Bank retains to ship, transport, and/or store Backup Tape(s) on which PI is or may be stored.

i. "WISP" shall mean a written information security program, as described in 201 C.M.R. 17.00 *et seq.*

#### IV. THE COMMONWEALTH'S ALLEGATIONS

8. The Commonwealth's allegations stem from the Incident in late March 2012, when a Bank employee placed a locked canvas bag containing two of the Bank's Backup Tapes on a secure loading dock of the Bank's Haverhill, Massachusetts office for pick-up and transport by a third-party service provider to the Bank's Springfield, Massachusetts office. The Commonwealth alleges that the Backup Tapes and the Bank's information stored on them were not encrypted as required by the Bank's then-existing WISP. To date, the Bank cannot confirm that the Backup Tapes arrived at its Springfield office or that the Backup Tapes have remained in the custody of an authorized person from the time they were placed on the Bank's Haverhill loading dock for transport in late March 2012.

9. The Commonwealth alleges that as of May 16, 2012, the Bank determined that it was unable to account for the location or custody of the Backup Tapes from the time they were placed on the Bank's Haverhill loading dock in late March 2012. The Commonwealth further alleges that at least as of May 16, 2012, the Bank knew or should have known, including through interviews with its employees concerning the general categories of information stored on the Backup Tapes, that the Backup Tapes contained unencrypted Personal Information of one or more Massachusetts residents. On October 5, 2012, the Bank notified the Attorney General under G.L. c. 93H of the Incident. On or about October 12, 2012, the Bank began notifying each of the over 90,000 affected Massachusetts residents of the Incident.

10. The Commonwealth alleges that the Bank violated G.L. c. 93H, § 3(b) and the Massachusetts Consumer Protection Act, G.L. c. 93A, § 2, by failing to give Notice of the Incident to the Attorney General's Office and to the affected Massachusetts residents (including through "substitute notice" as defined in G.L. c. 93H, § 1) "as soon as practicable and without unreasonable delay" when it knew or should have known of a Data Breach on or before May 16, 2012.

11. The Commonwealth further alleges that the Bank violated G.L. c. 93H, 201 C.M.R. 17.00 *et seq.*, and the Massachusetts Consumer Protection Act, G.L. c. 93A, § 2, including without limitation by: (a) not implementing its WISP throughout all of its Massachusetts offices with respect to the encryption of the Personal Information on the Backup Tapes and the secure, off-site transport of the Personal Information by a third-party service provider; (b) not encrypting the Personal Information stored on the Backup Tapes; (c) not identifying and/or assessing reasonably foreseeable risks to the security, confidentiality, and/or integrity of the Personal Information on the Backup Tapes; and (d) not taking reasonable steps to



select and retain a service provider capable of maintaining appropriate security measures to protect Personal Information entrusted to it by the Bank.

## V. THE BANK'S REPRESENTATIONS

12. The Bank denies that it has violated any Massachusetts laws or regulations in connection with the Incident, or that it engaged in any wrongdoing.

13. The Bank represents that on May 16, 2012, the Bank formally notified its federal regulators regarding the Incident. The Bank then immediately retained a forensics firm and undertook a four month effort, costing more than one million dollars, to recreate the data on the two Backup Tapes and determine whether they contained the Personal Information of any Massachusetts residents.

14. The Bank represents that the forensics firm produced to the Bank on July 20, 2012, a grid containing more than one million lines of raw data elements, including what could have been account numbers without any corresponding name or address. The Bank's internal team then worked to turn the raw data points into a list of individually identifiable persons to whom the Bank could send letters regarding the Incident, noting in each letter precisely which of the individual's data elements had been determined to be on the two Backup Tapes.

15. Prior to sending the letters to impacted Massachusetts residents in October 2012, the Bank notified the Attorney General on or about October 5, 2012.

16. The Bank represents that to date, there has been no evidence that the Backup Tapes are in the possession of an unauthorized person and no individuals whose Personal Information was on the Backup Tapes have identified any instances of fraud stemming from the Incident.

## VI. ASSURANCES

17. The Bank shall comply with G.L. c. 93H, including by providing Notice as soon as is practicable and without unreasonable delay, when it knows or has reason to know of a Data Breach, to the Commonwealth and to the Office of Consumer Affairs and Business Regulations, and to the affected Massachusetts resident(s), as required pursuant to G.L. c. 93H, § 3(b). The Bank shall provide Notice to the Commonwealth as soon as practicable and without unreasonable delay, notwithstanding that the Bank may not have provided or completed Notice to all affected Massachusetts residents, may not yet have all information necessary to provide Notice to all affected Massachusetts residents affected by the Data Breach, and/or may not have concluded its investigation of the full scope and nature of the Data Breach. The Bank shall promptly supplement its Notice to the Commonwealth as necessary if additional information is learned during the course of its investigation regarding the nature or scope of the Data Breach, including if additional residents are affected, to ensure that the Commonwealth is promptly notified of all information required under c. 93H, § 3(b).

18. The Bank shall comply with 201 C.M.R. 17.00, *et seq.*, including without limitation by:

- a. Maintaining a WISP that is compliant with 201 C.M.R. 17.03;
- b. Reviewing its security measures on at least an annual basis;
- c. Encrypting, to the extent technically feasible, all PI stored on Backup Tape(s);
- d. Taking reasonable steps to select and retain Service Provider(s) that are capable of maintaining appropriate security measures to protect any PI transferred or entrusted to the Service Provider by the Bank, consistent with 201 C.M.R. 17.00 *et seq.* and any applicable federal laws and regulations, and

- e. Requiring its Service Providers by contract to implement and maintain appropriate security measures with respect to PI, consistent with 201 C.M.R. 17.00 *et seq.* and all applicable federal laws and regulations.
19. The Bank shall, for a period of five (5) years following the Effective Date:
- a. Request and review its Transportation Service Providers' policies and procedures concerning the handling, shipping, transporting, tracking, and storing of PI to ensure reasonable safeguards are in place to protect PI entrusted or transferred by the Bank to such Transportation Service Provider;
  - b. Make reasonable inquiry into the security practices and policies of its Transportation Service Providers to understand the type of administrative, technical, and physical safeguards used by the Transportation Service Providers to protect PI entrusted or transferred to it by the Bank;
  - c. Request and review its Transportation Service Providers' policies and procedures for training its employees regarding the handling, transportation, tracking, and storing of PI pursuant to state and federal law;
  - d. Obtain and review a copy of its Transportation Service Providers' WISPs, to the extent such WISPs are required by law;
  - e. Maintain a written copy of all agreements with Transportation Service Providers;
  - f. Ensure that its Transportation Service Providers are aware when they are in possession of PI transferred or entrusted to them by the Bank, prior to their taking possession of the PI;

- g. Train all Bank personnel who have authority to enter into agreements with Transportation Service Providers as to the requirements of this paragraph; and
- h. Provide to the Attorney General a copy of a standardized Service Provider agreement that the Bank uses for its Transportation Service Provider(s) within thirty (30) days of the Effective Date.

20. The Bank shall:

- a. Within six (6) months of the Effective Date, perform a compliance review, consistent with any applicable law(s) and regulation(s), that reviews and assesses:
  - i. The Bank's WISP and the Bank's compliance with its WISP; and
  - ii. The Bank's implementation and compliance with the terms of this Assurance;
- b. Within three (3) months of the conclusion of the compliance review described in Paragraph 20(a), take all corrective actions that the Bank deems in good faith are necessary to bring the Bank into compliance with its WISP and this Assurance; and
- c. Provide a written description to the Commonwealth within one (1) month of the completion of all corrective actions taken pursuant to Paragraph 20(b) that details the methods used to conduct the compliance review and the results of the compliance review described in Paragraph 20(a) and the corrective actions taken (if any) as described in Paragraph 20(b).

21. For a period of three (3) years following the Effective Date, the Bank shall continue to maintain measures pursuant to its existing fraud detection systems to monitor



instances of unauthorized acquisition or unauthorized use of Personal Information involved in the Incident. If its fraud detection systems indicate any instance(s) of unauthorized acquisition or unauthorized use of the Personal Information related to the Incident, TD Bank, N.A. shall notify the Attorney General pursuant to paragraph 17 of this Assurance of Discontinuance.

22. The Bank shall inform its board of directors of the resolution of this matter and provide a copy of this Assurance of Discontinuance to the board of directors at the Bank's next regular meeting of the board of directors during which the Bank's Chief Compliance Officer gives an update on privacy and information security matters. Upon the Effective Date, this Assurance of Discontinuance shall also be provided to the Bank's primary privacy officer for purposes of disseminating the requirements of this Assurance of Discontinuance to those managers and other personnel within the Bank who negotiate with or utilize Transportation Service Providers, or to other personnel as necessary to carry out the terms of this Assurance.

23. For a period of five (5) years after the Effective Date, the Bank shall promptly provide a copy of this Assurance of Discontinuance to any successors or assigns resulting from a merger or sale of substantially all of the Bank's assets, and the provisions of this Assurance shall be binding thereon.

24. The Bank shall cooperate with all reasonable inquiries and requests from the Office of the Attorney General regarding implementation of the terms contained within this Assurance of Discontinuance.

## **VII. MONETARY PAYMENT**

25. The Bank hereby agrees to pay to the Commonwealth, on or prior to the Effective Date, a total settlement in the amount of \$825,000. This total settlement amount shall consist of a monetary payment by the Bank to the Commonwealth in the amount of \$625,000, which shall be allocated as follows: (1) \$325,000 as civil penalties pursuant to G.L. c. 93A, § 4, (2) \$75,000

as attorney's fees and costs pursuant to G.L. c. 93A, § 4, and (3) \$225,000 as a contribution to a fund to be used at the sole discretion of the Attorney General to promote education and/or to local consumer aid programs, pursuant to G.L. c. 12 § 11G. In satisfaction of the remainder of the total settlement amount, the Commonwealth has granted the Bank a \$200,000 credit based on its submission of satisfactory proof of the purchase and implementation of additional technology and other security controls and related services designed to protect the Personal Information maintained by the Bank.

26. Payment shall be made by wire transfer to the Commonwealth, pursuant to instructions to be provided to the Bank by the Attorney General.

#### VIII. RELEASE

27. This Assurance of Discontinuance resolves all existing civil claims the Attorney General may have against the Bank, stemming from the alleged violations of G.L. c. 93H, 201 C.M.R. 17.00 *et seq.*, and G.L. c. 93A, as described in this Assurance of Discontinuance. This Assurance of Discontinuance does not resolve, settle or otherwise affect any other actual or potential claims against the Bank, including, without limitation: any potential claims the Commonwealth may have against the Bank that do not arise from the Incident; claims arising from conduct occurring after the Effective Date; any contractual or administrative claims by any agency, board, authority or instrumentality of the Commonwealth other than the Attorney General; claims by any person or entity other than the Attorney General; claims that may be brought by the Attorney General against any other person or party; or any claims that are not civil in nature.

## IX. NOTICES

28. All notices and documents required by this Assurance of Discontinuance shall be provided in writing to the parties as follows:

A. If to the Attorney General:

Sara Cable  
Assistant Attorney General  
Consumer Protection Division  
Office of the Attorney General  
One Ashburton Place, 18<sup>th</sup> Floor  
Boston, MA 02108  
(617) 727-2200  
sara.cable@state.ma.us

B. If to TD Bank, N.A.:

Heather Egan Sussman, Esq.  
McDermott Will & Emery LLP  
28 State Street  
Boston, MA 02109  
(617) 535-4177  
hsussman@mwe.com

## X. MISCELLANEOUS

29. This Assurance of Discontinuance shall be filed in the Superior Court of Suffolk County. Pursuant to G.L. c. 93A, § 5, a violation of this Assurance of Discontinuance shall constitute prima facie evidence of a violation of G.L. c. 93A, § 2 in any subsequent proceeding brought by the Attorney General.

30. The Bank shall not form or knowingly affiliate with a separate person, entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited in this Assurance of Discontinuance or for any other purpose which would otherwise circumvent any part of this Assurance of Discontinuance.

31. Nothing in this Assurance of Discontinuance shall relieve the Bank of any obligation to comply with all applicable federal, state, and local laws, regulations, rules, and permits.

32. If the Attorney General determines that the Bank has not complied with the terms of this Assurance of Discontinuance and if, in the Attorney General's sole discretion, it determines that the failure to comply does not present an immediate threat to the health or safety of the citizens of the Commonwealth, the Attorney General shall not bring any action to enforce an alleged violation of this Assurance of Discontinuance without first providing the Bank with at least fourteen (14) days' written notice in accordance with Paragraph 28 that identifies with reasonable particularity the conduct that is alleged to violate this Assurance of Discontinuance.

33. Consent to this Assurance of Discontinuance does not constitute an admission by the Bank of any wrongdoing.

34. Consent to this Assurance of Discontinuance does not constitute an approval or sanction by the Commonwealth of any of the Bank's business acts and practices, or agreement with the Bank's representations made herein, and the Bank shall not represent this Assurance of Discontinuance as such an approval, sanction, or agreement. The Bank further understands that any failure by the Attorney General to take any action in response to any information submitted pursuant to the Assurance shall not be construed as an approval or sanction of any representations, acts or practices indicated by such information, nor shall it preclude action thereon at a later date.

35. The Superior Court of Massachusetts shall retain jurisdiction over this Assurance of Discontinuance, and the provisions of this Assurance of Discontinuance shall be construed in accordance with the laws of the Commonwealth of Massachusetts.



36. The provisions of this Assurance of Discontinuance shall be severable and should any provisions be declared by a court of competent jurisdiction to be unenforceable, the other provisions of this Assurance of Discontinuance shall remain in full force and effect.

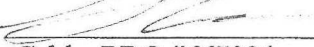
37. This Assurance of Discontinuance contains the complete agreement between the parties. The parties have made no promises, representations, or warranties other than those in this Assurance of Discontinuance. This Assurance of Discontinuance supersedes all prior communications, discussions, or understandings, if any, of the parties, whether written or oral. This Assurance of Discontinuance can be modified or supplemented only by written memorandum signed by the parties.

38. T.D. Bank, N.A. is represented by and has consulted with counsel, Steven A. Baddour, Marcos Daniel Jimenez, and Heather Egan Sussman of McDermott Will & Emery LLP, in connection with its decision to enter into this Assurance of Discontinuance.

39. The undersigned, Albert M. Raymond, represents that he is duly authorized to execute this Assurance of Discontinuance on behalf of TD Bank, N.A. and to bind TD Bank, N.A. to all of its provisions, and that on behalf of TD Bank, N.A., he voluntarily enters into this Assurance of Discontinuance.

COMMONWEALTH OF MASSACHUSETTS

MARTHA COAKLEY  
ATTORNEY GENERAL

By:   
Sara Cable, BBO #667084  
Assistant Attorney General  
Consumer Protection Division  
One Ashburton Place  
Boston, MA 02108  
(617) 727-2200

Dated: December 8, 2014

TD BANK, N.A.

By: 

Albert M. Raymond  
U.S. Chief Privacy Officer  
2059 Springdale Road  
Cherry Hill, NJ 08003

Dated: 12-3-14