**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MINNESOTA**

| | | |
|---|---|---|
| HARBORONE BANK, MUTUAL BANK and PITTSFIELD COOPERATIVE BANK, individually and on behalf of a class of similarly situated financial institutions, | : | Case No: |
| Plaintiffs, | : | **CLASS ACTION COMPLAINT** |
| v. | : | JURY TRIAL DEMANDED |
| TARGET CORPORATION, AND TRUSTWAVE HOLDINGS, INC. | : | |
| Defendants. | : | |

Plaintiffs HarborOne Bank, Mutual Bank and Pittsfield Cooperative Bank, through their undersigned counsel, individually and on behalf of a class of similarly situated financial institutions, file this Class Action Complaint against Defendants Target Corporation ("Target") and Trustwave Holdings, Inc. ("Trustwave" and collectively, "Defendants").

## NATURE OF THE ACTION

1. This is a class action on behalf of banks and other financial institutions who suffered injury as a result of a security breach compromising Target store customers' names, credit and debit card numbers, card expiration dates, personal identification numbers ("PINs"), and card verification values ("CVVs") (hereinafter the "Target Data Breach"), forcing these institutions to: (a) cancel or reissue any access device affected by the Target Data Breach; (b) close any deposit, transaction, checking, or other accounts

affected by the breach, including but not limited to stopping payments or blocking transactions with respect to the accounts; (c) open or reopen any deposit, transaction, checking, or other accounts affected by the Target Data Breach; (d) refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Target Data Breach; or (e) notify cardholders affected by the Target Data Breach.

2. As alleged herein, the injuries to Plaintiffs and the Class were caused by Defendants' failure to maintain adequate computer data security of customer information, including credit and debit card data, as well as personally identifying information. Upon information and belief, Defendants also failed to remove or delete card security code data, the PIN verification code number, and/or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction, in express violation of Minn. Stat. § 325E.64, Subd. 2.

3. As a result of Defendants' wrongful actions, customer information was stolen from Target's computer network. Millions of Target's customers have had their personal financial information compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Additionally, Plaintiffs and members of the Class have incurred and will continue to incur significant costs associated with, among other things, notifying their customers of issues related to the Target Data Breach, closing out and opening new customer accounts, reissuing customers' cards, and/or refunding customers' losses resulting from the unauthorized use of their accounts.

4. Plaintiffs and the Class seek to recover damages caused by Defendants' unfair and/or deceptive acts or practices in violation of Minn. Stat. § 325F.69, Subd. 1 (Count I); acts in violation of Minn. Stat. § 325E.64 (Count II), and negligence (Count III).

5. Plaintiffs and the Class also seek a finding that Defendants improperly retained customer data and injunctive relief enjoining Defendants from such improper retention of information.

## JURISDICTION AND VENUE

6. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class defined below, who reside in a different state than Defendants. All named Plaintiffs are citizens of Massachusetts. Defendant Target is a citizen of Minnesota. Defendant Trustwave is a citizen of Illinois (state of principal place of business) and Delaware (state of incorporation).

7. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because Defendant Target resides in this judicial district, regularly transacts business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

## PARTIES

8. Plaintiff HarborOne Bank is a savings bank with its principal place of business located at 68 Legion Parkway, Brockton, Massachusetts 02301.

9. Plaintiff Mutual Bank is a savings bank with its principal place of business located at 570 Washington Street, Whitman, Massachusetts 02382.

10. Plaintiff Pittsfield Cooperative Bank is a savings bank with its principal place of business located at 70 South Street, Pittsfield, Massachusetts 01202-1076.

11. Defendant Target Corporation is a Minnesota corporation with its principal place of business located in Minneapolis, Minnesota. Target operates a chain of retail stores that sell merchandise, including home goods, electronics, and clothing. Target owns over 1,790 stores in the United States.

12. Defendant Trustwave Holdings, Inc. is a Delaware corporation with its principal place of business located at 70 W. Madison St., Suite 1050, Chicago, Illinois 60602. Trustwave provides data security services to a wide range of businesses, including Target Corporation.

## FACTUAL BACKGROUND

### The Target Data Breach Unravels

13. On December 18, 2013, respected security blogger, Brian Krebs reported that "Target is investigating a data breach potentially involving millions of customer credit and debit card records." *See* Krebs on Security December 18, 2013, Blog Post (*available at* http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/).[1]

14. Following Mr. Krebs's announcement, on December 19, 2013, Target issued a statement confirming that a security breach occurred and asserted that 40 million

[1] All cited websites were last visited on March 26, 2014.

credit and debit card accounts may have been impacted between November 27, 2013, and December 15, 2013. *See* "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores" (*available at* http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores) (hereinafter "December 19, 2013, Press Release").

15. Not until December 20, 2013, over three weeks after the data breach began, did Target reach out to its impacted customers to inform them of the issue. *See* December 20, 2013, Target Email to Customers (*available at* https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca).

16. In the December 20, 2013, Target Email to Customers, Target admitted that the security breach "included customer name, credit or debit card number, and the card's expiration date and CVV." *See id.*

17. Target further acknowledged that "encrypted debit card PIN data was among the information stolen when its systems were breached during the peak holiday shopping period." Target noted that "its investigation now shows that encrypted PIN data was 'removed' from its systems." *See* "Target Says Encrypted PIN Data Taken in Breach," THE WALL STREET JOURNAL, Dec. 27, 2013 (*available at* http://online.wsj.com/news/articles/SB10001424052702303345104579284440022934198?cb=logged0.0365547111723572).

18. Then, on January 10, 2014, Target made another announcement, this time conceding that its "investigation has determined that the stolen information includes

names, mailing addresses, phone numbers or email addresses for up to 70 million individuals." *See* "Target Provides Update on Data Breach and Financial Performance" (*available at* http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance) (hereinafter "January 10, 2014, Target Press Release").

19. Reports have shown that the information for the 70 million individuals was stored separately from the 40 million credit and debit card accounts that Target previously admitted was impacted. *See* "Target Now Says 70 Million People Hit in Data Breach," THE WALL STREET JOURNAL, Jan. 10, 2014 (*available at* http://online.wsj.com/news/articles/SB10001424052702303754404579312232546392464).

20. In combination with the initially reported 40 million customers whose credit and debit card accounts were affected, the Target data breach impacted approximately up to 110 million consumers. *See id.*

21. As a result of Target's wrongful conduct, sensitive customer information was accessed from Target's computer systems. Indeed, "[f]raud experts said the information stolen from Target's systems quickly flooded the black market. On Dec. 11, 2013, shortly after hackers first breached Target, Easy Solutions, a company that tracks fraud, noticed a 10 to twentyfold increase in the number of high-value stolen cards on black market websites, from nearly every bank and credit union." *See* "For Target, the Breach Numbers Grow," THE NEW YORK TIMES, Jan. 10, 2014 (*available at* http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0 ).

**Defendants Missed Multiple Opportunities to Prevent or Stop the Data Theft**

22. Recent reports indicate that Defendants received numerous alerts about the breach from data security software installed by one of Target's vendors, FireEye, as the attack was occurring. Despite these warnings, and alerts from other data security vendors employed by Target, Defendants took no action.

23. An investigation by *Bloomberg Businessweek*, citing conversations with "10 former Target employees familiar with the company's data security operation, as well as eight people with specific knowledge of the hack and its aftermath," found that FireEye's malware detection program "worked beautifully. But then, Target stood by as 40 million credit card numbers—and 70 million addresses, phone numbers, and other pieces of personal information—gushed out of its mainframes." The article goes on to describe the nature of Target's inaction in detail:

> In testimony before Congress, Target has said that it was only after the U.S. Department of Justice notified the retailer about the breach in mid-December that company investigators went back to figure out what happened. What it hasn't publicly revealed: Poring over computer logs, Target found FireEye's alerts from Nov. 30 and more from Dec. 2, when hackers installed yet another version of the malware. Not only should those alarms have been impossible to miss, they went off early enough that the hackers hadn't begun transmitting the stolen card data out of Target's network. Had the company's security team responded when it was supposed to, the theft that has since engulfed Target, touched as many as one in three American consumers, and led to an international manhunt for the hackers never would have happened at all.
>
> * * *
>
> On Nov. 30, according to a person who has consulted on Target's investigation but is not authorized to speak on the record, the hackers deployed their custom-made code, triggering a FireEye alert that indicated unfamiliar malware: "malware.binary." Details soon followed, including addresses for the servers where the hackers wanted their stolen data to be sent. As the hackers inserted more

> versions of the same malware (they may have used as many as five, security researchers say), the security system sent out more alerts, each the most urgent on FireEye's graded scale, says the person who has consulted on Target's probe.
>
> The breach could have been stopped there without human intervention. The system has an option to automatically delete malware as it's detected. But according to two people who audited FireEye's performance after the breach, Target's security team turned that function off.
>
> * * *
>
> Even the company's antivirus system, Symantec Endpoint Protection, identified suspicious behavior over several days around Thanksgiving—pointing to the same server identified by the FireEye alerts. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee. If Target had had a firm grasp on its network security environment, he adds, "they absolutely would have observed this behavior occurring on its network."

*See* Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," BLOOMBERG BUSINESSWEEK, Mar. 13, 2014 (*available at* http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data).

24. Echoing the findings by *Businessweek* and others, a preliminary report prepared for the U.S. Senate Committee on Commerce, Science, and Transportation presented the following summary conclusions:

> Target gave network access to a third-party vendor, a small Pennsylvania HVAC company, which did not appear to follow broadly accepted information security practices. The vendor's weak security allowed the attackers to gain a foothold in Target's network.
>
> Target appears to have failed to respond to multiple automated warnings from the company's anti-intrusion software that the attackers were installing malware on Target's system.

> Attackers who infiltrated Target's network with a vendor credential appear to have successfully moved from less sensitive areas of Target's network to areas storing consumer data, suggesting that Target failed to properly isolate its most sensitive network assets.
>
> Target appears to have failed to respond to multiple warnings from the company's anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network.

*See* U.S. Senate, Committee on Commerce, Science, and Transportation (Majority Staff Report), *A "Kill Chain" Analysis of the 2013 Target Data Breach*, at 1, Mar. 26, 2014 (*available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883).

25. According to the testimony of Target's CFO before the Senate Committee on the Judiciary, Target had been certified in September 2013 as compliant with the Payment Card Industry Data Security Standards (PCI-DSS), which credit card companies require before allowing merchants to process credit and debit card payments. *Id.* at 7.

26. Upon information and belief, the September 2013 compliance certification was made by Defendant Trustwave.

27. The initial stages of the attack may have started as early as November 12 or 15, 2013, or almost a month before Target was informed of the attack by the Department of Justice. *Id.* at 3.

28. The attackers conducted the data-collection part of the attack by installing malware on Target's Point of Sale terminals. This malware utilized a so-called "RAM scraping" attack, which allowed for the collection of unencrypted, plaintext data as it

passed through the infected POS machine's memory before transfer to the company's payment processing provider. *Id.* at 2.

29. The attackers uploaded five variations of a malware program, designed to help the attackers move data through Target's systems, between November 30 and December 3, 2013. *Id.*

30. The FireEye system generated urgent alerts for Target each time the malware was uploaded. *Id.*

31. The attackers initially collected the stolen data on Target's own servers before "exfiltrating" 11 gigabytes worth of data to a Russia-based server, and possibly other locations including Miami and Brazil, over the course of two weeks. *Id.* at 3-4.

32. As a direct and proximate result of the Target Data Breach, Plaintiffs and members of the Class have been damaged, because Target's wrongful conduct has caused Class members to incur significant losses associated with credit and debit card cancellation and/or reissuance; customer reimbursement for fraud losses; lost interest and transaction fees; lost customers; administrative expenses associated with monitoring and preventing fraud and administrative expenses in dealing with customer confusion; and claims alleging fraudulent activity.

**Target Data Retention Practices Violate Applicable Laws**

33. Defendants, at all times relevant to this action, represented and had a duty to Plaintiffs and members of the Class to: (a) properly secure credit card magnetic stripe information; (b) not retain or store such information subsequent to authorization of a transaction; and (c) not disclose such information to unauthorized third parties.

34. As outlined in numerous reports, Defendants retained magnetic stripe information and data from millions of credit and debit cards issued by Plaintiffs and members of the Class, or allowed such information to be stored on Target's servers.

35. Defendants negligently allowed credit card magnetic stripe information to be compromised.

36. Upon information and belief, Defendants negligently utilized a computer system that retained, stored, and/or disclosed credit card magnetic stripe information (or allowed such information to be retained, stored, and/or disclosed).

37. Data from the magnetic stripe on millions of credit cards, issued by banks and other financial institutions to their customers and members, was used by those customers at Target stores, and was accessed or obtained by third parties from Defendants.

38. Third parties were able to access, obtain, and use the credit card magnetic stripe information to fraudulently make transactions and to sell, transfer, use, or attempt to use such information for fraudulent purposes.

39. As a result of the events detailed herein, Plaintiffs and members of the Class have been and continue to be forced to protect their customers and avoid fraud losses by cancelling and reissuing cards with new account numbers and magnetic stripe information.

40. As a result of Defendants' failure to safeguard customer information, to date, Plaintiff HarborOne Bank has been forced to cancel and reissue approximately

4,369 debit cards and credit cards and has incurred additional costs related to notifying and reissuing cards to its customers.

41. As a result of Defendants' failure to safeguard customer information, to date, Plaintiff Mutual Bank has been forced to cancel and reissue approximately 1,359 debit and credit cards and incurred related costs for notification and resissuance of cards to its customers. Plaintiff Mutual Bank incurred additional losses and expenses as a result of its efforts to prevent at-risk cards from being used fraudulently.

42. As a result of Defendants' failure to safeguard customer information, to date, Plaintiff Pittsfield Cooperative Bank has been forced to cancel and reissue approximately 251 debit and credit cards and incur related costs for notification and resissuance of cards to its customers. Plaintiff Pittsfield Cooperative Bank incurred additional losses and expenses as a result of its efforts to prevent at-risk cards from being used fraudulently.

43. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiffs and members of the Class. Moreover, as a result of the events detailed herein, Plaintiffs and members of the Class suffered losses resulting from the Target Data Breach related to: (a) reimbursement of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as cancelling compromised cards and purchasing and mailing new cards to their customers.

44. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

## CLASS ACTION ALLEGATIONS

45. Plaintiffs bring this action individually and on behalf of all other financial institutions similarly situated pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and Fed. R. Civ. P. 23.2. The proposed class is defined as:

> All banks and other financial institutions that are members of the Massachusetts Bankers Association who as a result of the Target Data Breach, were forced to communicate with their customers, close out or open new customer accounts, reissue credit and/or debit cards, absorb unauthorized charges to customers' accounts, or were in any other way forced to pay for issues related to the Target Data Breach (the "Class").

46. Plaintiffs are all members of the Class they seek to represent.

47. The Class is so numerous that joinder of all members is impracticable.

48. The members of the Class are readily ascertainable.

49. Plaintiffs' claims are typical of the claims of all members of the Class.

50. The conduct of Defendants has caused injury to Plaintiffs and members of the Class.

51. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendants.

52. Plaintiffs will fairly and adequately represent the interests of the Class.

53. Defendants have acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

54. Plaintiffs are represented by experienced counsel who are qualified to litigate this case.

55. Common questions of law and fact predominate over individualized questions. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

56. There are questions of law and fact common to all members of the Class, the answers to which will advance the resolution of the claims of the Class members and that include, without limitation:

a) Whether Defendants failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;

b) Whether the conduct of Defendants resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;

c) Whether Defendants improperly retained customer personal and financial information or allowed such information to be retained on its systems despite representations that it would not keep such information;

d) Whether Defendants disclosed, either directly or indirectly, the private financial information of customers;

e) Whether Defendants violated Minn. Stat. § 325E.64;

f) Whether Defendants engaged in unfair and deceptive acts or practices as set forth in Minn. Stat. § 325F.69, Subd. 1;

g) Whether Plaintiffs and members of the Class have been injured by Defendants' violations of Minnesota law;

h) Whether Plaintiffs and members of the Class are entitled to injunctive relief; and

**i)** Whether Plaintiffs and members of the Class are entitled to damages and the measure of such damages.

**COUNT ONE**
**VIOLATION OF MINN. STAT. § 325F.69, SUBD. 1**

57. Plaintiffs incorporate and re-alleges each and every allegation contained above as if fully set forth herein.

58. Target and Trustwave are engaged in trade or commerce in the State of Minnesota.

59. Plaintiffs and members of the Class are banks and financial institutions engaged in trade or commerce.

60. Upon information and belief, Defendants' computer systems that process and store information related to credit and debit card transactions on which customer data was retained and from which customer data was improperly accessed are located at in Minneapolis, Minnesota.

61. Defendants' practice of retaining, failing to safeguard, and allowing access to confidential customer data constitutes deceptive acts and unfair trade practices within the meaning of Minn. Stat. § 325F.69, Subd. 1.

62. Defendants' actions in connection with their failures to adequately protect Plaintiffs' customers' data, and their misconduct regarding the confidential debit and credit cardholders' information constitute deceptive acts and unfair trade practices, having a direct and substantial effect in Minnesota and throughout the United States causing substantial damages to Plaintiffs and members of the Class.

**COUNT TWO**
**VIOLATION OF MINN. STAT. § 325E.64**

63. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

64. Defendants had a duty under Minn. Stat. § 325E.64, Subd. 2, to provide notification of the data breach to Plaintiffs and members of the Class. The statute specifically requires that:

> No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

65. Minn. Stat. § 325E.64, Subd. 3, details Defendants' responsibilities following the breach. Specifically, this subdivision provides that:

> Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:
>
> (1) the cancellation or reissuance of any access device affected by the breach;
>
> (2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;
>
> (3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;
>
> (4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and
>
> (5) the notification of cardholders affected by the breach.
>
> The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

66. Defendants breached the duties they owed to Plaintiffs and members of the Class under Minn. Stat. § 325E.64 by failing to remove or delete card security code data,

the PIN verification code number, and/or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

67. As a direct and proximate result of Defendants' breach of its duties under Minn. Stat. § 325E.64, Plaintiffs and members of the Class have suffered substantial losses as detailed herein.

## COUNT THREE
## NEGLIGENCE

68. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

69. Defendants owed a duty to Plaintiffs and the Class to use and exercise reasonable and due care in obtaining and retaining Plaintiffs' customers' personal and financial information.

70. Defendants owed a duty to Plaintiffs and the Class to provide adequate security to protect Plaintiffs' customers' personal and financial information.

71. Defendants breached their duties, by (1) retaining customer data or allowing such data to be retained on Target's servers beyond the period allowed under Minn. Stat. § 325E.64; (2) allowing an unlawful intrusion into its computer system; (3) failing to protect against such an intrusion; and (4) allowing the personal and financial information of customers from Plaintiffs and the Class to be accessed by third parties.

72. Defendants knew, or should have known, of the risks inherent in retaining such information, and the importance of providing adequate security.

73. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and the Class have suffered substantial losses as detailed herein.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that this Court enter a judgment against Defendants and in favor of Plaintiffs and the Class and award the following relief:

A. That this action be certified as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiffs as representatives of the Class and Plaintiffs' counsel as counsel for the Class;

B. Monetary damages;

C. Damages pursuant to Defendants' willful and knowing violations of Minn. Stat. § 325F.69, Subd. 1;

D. A finding that Defendants violated Minn. Stat. § 325E.64 and an order enjoining Defendants from any further improper retention of customer data;

E. Reasonable attorneys' fees and expenses, including those related to experts and consultants;

F. Costs;

G. Pre and post judgment interest; and

H. Such other relief as this Court may deem just and proper.

## JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs, individually and on behalf of the Class, demand a trial by jury for all issues so triable.

DATED: March 28, 2014

Respectfully submitted,

LOCKRIDGE GRINDAL NAUEN P.L.L.P.

By: /s/ Karen H. Riebel

Karen Hanson Riebel (#0219770)
Richard A. Lockridge (#64117)
Gregg M. Fishbein (#202009)
Robert K. Shelquist (#21310X)
Kate M. Baxter-Kauf (#0392037)
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
ralockridge@locklaw.com
gmfishbein@locklaw.com
rkshelquist@locklaw.com
kmbaxter-kauf@locklaw.com

Gary F. Lynch
R. Bruce Carlson
Jamisen Etzel
Sunshine Fellows
CARLSON LYNCH LTD
PNC Park
115 Federal Street, Suite 210
Pittsburgh, PA 15212
Tel: (412) 322-9243
Fax: (412) 231-0246

Benjamin J. Sweet
Edwin J. Kilpela, Jr.
DEL SOLE CAVANAUGH STROYD LLC
200 First Avenue, Suite 300
Pittsburgh, PA 15222
Tel: (412) 261-2393
Fax: (412) 261-2110

Shanon J. Carson
Alexandra L. Koropey
BERGER & MONTAGUE, P.C.
1622 Locust Street
Philadelphia, PA 19103
Tel: (215) 875-4656
Fax: (215) 875-4604