IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

FIRST CHOICE FEDERAL CREDIT UNION and FINANCIAL HORIZONS CREDIT UNION, individually and on behalf of all others similarly situated, Plaintiffs, v. SLIM CD, INC., Defendant.	Case No. 2:25-cv-01088 **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Financial Institution Plaintiffs First Choice Federal Credit Union and Financial Horizons Credit Union ("Plaintiffs"), individually and on behalf of the Class (defined below), based on personal knowledge as to themselves and their own acts, on information and belief where indicated, and upon investigation of counsel as to all other matters, bring this putative class action against Defendant Slim CD, Inc. ("Slim CD" or "Defendant") and allege as follows:

INTRODUCTION

1. Plaintiffs bring this class action on behalf of a class of financial institutions that suffered, and continue to suffer, harm as a direct result of Slim CD's conscious failure to take adequate and reasonable measures to protect Plaintiffs' and their customers' personal and financial data.

2. Slim CD's negligent actions exposed highly sensitive Payment Card Data ("PCD"), including cardholder names, credit card numbers, card expiration dates, and other critical payment card details, belonging to approximately 1.7 million consumers. This data was left vulnerable and accessible to hackers between August 17, 2023 and June 15, 2024. As a direct consequence,

Plaintiffs have incurred significant damages, including, but not limited to: costs associated with replacing compromised payment cards, covering fraudulent transactions, and expenses related to customer service, increased fraud monitoring, and operational disruptions.[1]

3. Slim CD is a payment processing gateway that facilitates electronic credit and debit card transactions for numerous U.S.-based merchants across various industries, including retail, hospitality, and restaurants through web-based terminals, and mobile and/or desktop applications.

4. Due to the nature of its business, Slim CD knowingly collects, processes, and stores large quantities of sensitive financial information. Consequently, Slim CD owed an explicit duty to Plaintiffs and the Class to adequately secure such information from unauthorized access and exfiltration.

5. Despite its obligations under industry standards, including the Payment Card Industry Data Security Standards ("PCI DSS") and Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Slim CD failed to adequately safeguard Plaintiffs' customers' PCD, directly resulting in the Data Breach.

6. On or about September 6, 2024, Slim CD publicly acknowledged that unauthorized third parties gained access to its computer systems over an extended period of time from August 17, 2023 to June 15, 2024.[2] Slim CD further stated that the access may have enabled an unauthorized actor to view or obtain certain credit card information between June 14, 2024, and June 15, 2024 (the "Data Breach").[3] Despite the severity of the breach, Slim CD failed to provide

---

[1] Bill Toulas, *Payment gateway data breach affects 1.7 million credit card owners*, BleepingComputer (Sept. 9, 2024), https://www.bleepingcomputer.com/news/security/payment-gateway-data-breach-affects-17-million-credit-card-owners/.

[2] *Notice of Data Privacy Event*, Slim CD, https://stats.slimcd.com/slimcddata.pdf (last accessed July 22, 2025).

[3] *Id.*

adequate and timely notification to affected institutions and failed to disclose specific details about the vulnerabilities exploited, measures taken to rectify security shortcomings, and assurances that stolen data had been secured or destroyed.

7. Slim CD's failure to protect sensitive PCD has caused immediate and substantial financial damage to Plaintiffs and the Class, including significant costs incurred from reissuing compromised payment cards, reimbursing customers for fraudulent charges, managing heightened fraud detection and monitoring efforts, and enduring substantial operational and reputational harm.

8. As a direct and proximate result of Slim CD's negligence, Plaintiffs' customers' PCD is now readily available to cybercriminals and has been actively trafficked on illicit dark web marketplaces, substantially increasing the risk of ongoing and future fraud.

9. Slim CD's management consciously disregarded specific warnings and known risks associated with its deficient data security infrastructure, thus facilitating the unauthorized access and exfiltration of highly sensitive PCD affecting approximately 1.7 million individuals and their payment card issuers. This Data Breach represents a significant incident with substantial negative implications for the financial institutions forced to address the fallout.

10. This Data Breach shocks the conscience. Defendant Slim CD fully understood its duties to protect the confidentiality, accuracy, and integrity of PCD. Slim CD understood that a data breach was a foreseeable and legitimate risk, and that if such an event occurred, the consequences for financial institutions would be severe. Yet, Slim CD failed to implement basic, industry-standard data security measures that would have protected PCD.

11. Slim CD was on heightened notice of the risks of payment card data breaches and the consequences of deficient cybersecurity practices. Specifically, as an entity whose business

offers products and services designed to process credit and debit card transactions, Slim CD knew or should have known that such PCD possess a heightened risk of theft by cybercriminals.

12. Publicly available guidance from the Federal Trade Commission ("FTC") and the Payment Card Industry Security Standards Council, including PCI DSS standards, put Slim CD on clear notice of its duty to implement robust cybersecurity protocols. Moreover, Slim CD's own core business model, as a payment processing gateway handling credit card transactions for merchants nationwide, requires it to maintain high-level data security. Slim CD failed to take precautions that were known and readily available, allowing threat actors prolonged access to its systems between August 17, 2023 and June 15, 2024.

13. Following the public disclosure of the breach in September 2024, Slim CD failed to provide full transparency to financial institutions. Unlike industry leaders that respond to similar breaches by immediately implementing corrective measures and adopting heightened security standards such as multi-factor authentication and penetration testing, Slim CD did not commit to such post-breach reforms. To date, it has not confirmed that the stolen data has been securely recovered or destroyed, nor has it communicated any definitive changes to its internal controls to prevent future breaches.

14. The Data Breach was a direct and proximate result of Slim CD's decision to disregard recommended cybersecurity measures. These decisions left the PCD of Plaintiffs' customers unencrypted, unsegregated, and fully accessible to cybercriminals, who were able to exfiltrate sensitive payment information over a ten-month period. Had Slim CD adopted reasonable, industry-standard security measures, including those outlined by the PCI DSS, it could have prevented the Data Breach and/or identified substantially sooner.

15. Plaintiffs and the Class have already borne, and will continue to bear, substantial costs due to Slim CD's negligence. These costs include, but are not limited to, the cancellation and reissuance of compromised payment cards, reimbursement of fraud losses, heightened fraud monitoring expenses, and customer service operations to address affected account holders' concerns.

16. In addition, Plaintiffs and the Class have incurred significant out-of-pocket costs in investigating and responding to the Data Breach. This includes increasing internal fraud detection protocols, evaluating and enhancing cybersecurity systems, communicating with customers, and preparing for the inevitable future misuse of the compromised PCD.

17. The risk of future harm remains real and imminent. Plaintiffs and the Class face an ongoing threat of fraudulent payment card activity, banking fraud, and reputational harm. These risks will persist as long as the stolen PCD remains in the hands of cybercriminals, requiring Plaintiffs to incur continued costs to reduce and mitigate these risks.

18. Plaintiffs, individually and on behalf of a nationwide class of similarly situated financial institutions, seek both monetary and injunctive relief. Plaintiffs assert claims for negligence, including negligence *per se* under the FTC Act and industry standards such as PCI DSS. Plaintiffs also seek declaratory relief requiring Slim CD to implement comprehensive cybersecurity measures in line with industry best practices to ensure this breach is not repeated.

PARTIES

Plaintiffs

19. Plaintiff First Choice Federal Credit Union ("FCFCU") is a federally-chartered credit union with a principal place of business in New Castle, Pennsylvania. Plaintiff Financial Horizons Credit Union received. On or around October 2024, FCFCU received a Compromised

Account Management System ("CAMS") alert, indicating that PCD, including customer names, addresses, payment account numbers ("PAN") data, and expiration dates had been exposed in the Data Breach. PAN is a unique payment card number (credit, debit, or prepaid cards, etc.) that identifies the issuer (financial institution) and the cardholder account. The PAN number is crucial for the identification of the issuer and the specific account within the issuer's systems. PANs are used across various card types including credit, debit, and prepaid cards, and are essential for facilitating electronic financial transactions. As a result of the Data Breach, FCFCU has suffered, and continues to suffer, injury, including, among other things, costs to cancel and reissue payment cards compromised in the Data Breach, costs associated with the time and expense associated with investigating the Data Breach, costs of fraud monitoring, and costs due to lost interest and transaction fees due to reduced payment card usage.

20. Plaintiff Financial Horizons Credit Union is a state-chartered credit union with a principal place of business in Hawthorne, Nevada. Plaintiff Financial Horizons Credit Union received. Beginning on or around August 2024 and again in June 2025, Visa issued a number of CAMS alerts to Financial Horizons Credit Union, indicating that PCD, including customer names, addresses and PAN data had been exposed in the Data Breach. PAN is a unique payment card number (credit, debit, or prepaid cards, etc.) that identifies the issuer (financial institution) and the cardholder account. The PAN number is crucial for the identification of the issuer and the specific account within the issuer's systems. PANs are used across various card types including credit, debit, and prepaid cards, and are essential for facilitating electronic financial transactions. As a result of the Data Breach, Financial Horizons Credit Union has suffered, and continues to suffer, injury, including, among other things, costs to cancel and reissue payment cards compromised in the Data Breach, costs to refund fraudulent charges, costs associated with the time and expense

associated with investigating the Data Breach, costs of fraud monitoring, and costs due to lost interest and transaction fees due to reduced payment card usage.

Defendant

21. Defendant Slim CD, Inc. is a Florida corporation with its principal place of business located at 610 N University Drive, Coral Springs, Florida 33071. Slim CD is a payment gateway and processing provider for merchants across the United States, handling electronic payment transactions, including those involving credit and debit cards.

22. Slim CD's role as a central processor of consumer payment card transactions places it in a position of significant responsibility with respect to the safeguarding of sensitive financial data. As alleged herein, Slim CD failed to implement reasonable and industry-standard measures to protect that data, leading to the exposure of vast amounts of PCD belonging to customers of Financial Institution Plaintiffs and Class Member.

23. Slim CD's responsibilities include, but are not limited to, ensuring compliance with PCI DSS, establishing and maintaining internal safeguards to prevent unauthorized access to stored payment card data, and conducting appropriate oversight of third-party systems and services used in connection with payment processing. Slim CD failed in each of these respects.

24. As set forth herein, Slim CD's inadequate data security infrastructure and disregard for established standards of care directly facilitated the prolonged and unauthorized access to sensitive Payment Card Data over a ten-month period. As a result, financial institutions have incurred substantial costs related to fraud remediation, customer protection, and operational response.

25. Plaintiffs bring this action against Slim CD alone, as Slim CD is the sole entity responsible for maintaining the systems that were compromised in the breach at issue. Slim CD's negligence and related statutory violations are the direct and proximate cause of Plaintiffs' injuries.

JURISDICTION AND VENUE

26. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d). The aggregated claims of the individual class members exceed the sum or value of $5,000,000 exclusive of interest and costs; the proposed class contains well over 100 members; and minimal diversity exists because at least one member of the Class is a citizen of a state different from Defendant Slim CD, Inc.

27. This Court has personal jurisdiction over Defendant because Defendant routinely conducts business in the Commonwealth where this district is located, has sufficient minimum contacts in this Commonwealth, and has intentionally availed itself of this jurisdiction by marketing and selling services, including the collection, processing, and storage of PCD for merchants in this Commonwealth and nationwide. Upon information and belief, some of the PCD collected and processed by Slim CD and ultimately compromised in the Data Breach is that of financial institutions located in this Commonwealth.

28. Venue is proper in the United States District Court for the Western District of Pennsylvania under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiffs' claims occurred within this District, and Defendant does business in this District.

FACTUAL ALLEGATIONS

A. Background on Electronic Debit and Credit Card Transactions and Requirements for Securing Data

29. Plaintiffs and the members of the Class are financial institutions that issue payment cards to their customers and are contractually and statutorily obligated to reimburse cardholders for fraudulent transactions and to absorb the operational costs of replacing compromised cards.[4]

[4] These cards include, for example, debit or credit cards branded with the Visa or MasterCard logo.

30. Slim CD processes payment card transactions on behalf of thousands of U.S. merchants. When a cardholder initiates a purchase, either online through an e-commerce platform integrated with Slim CD's gateway or in-store through a point-of-sale ("POS") terminal, Slim CD receives and transmits the cardholder's PCD, which includes the primary account number, expiration date, and other sensitive data elements.

31. The transaction flow is as follows: (1) the cardholder's PCD is captured at the merchant interface and transmitted to Slim CD; (2) Slim CD forwards an authorization request through a payment network (*e.g.*, Visa, Mastercard) to the issuing financial institution (one of the Plaintiffs or a Class member); (3) the issuing institution approves or declines the transaction and returns an authorization response via the same network; (4) Slim CD relays the response to the merchant, and, ultimately, the acquiring bank settles funds with the merchant while the issuing institution posts the transaction to the cardholder's account.

32. PCD is highly valuable to cybercriminals, who routinely exploit security weaknesses in payment environments. High-profile breaches at Equifax, Home Depot, Target, Wawa, Ticketmaster, and other entities illustrate the magnitude of risk and the significant remediation costs borne by financial institutions.

33. At all relevant times, Slim CD knew or should have known that it was a prime target for cyber-attacks. Industry guidance, including alerts from the PCI Security Standards Council and publications from the FTC, emphasized the need for robust security controls, continuous monitoring, and strict adherence to PCI DSS requirements.

34. Despite this knowledge, Slim CD failed to deploy basic security safeguards, such as encryption of stored card data, network segmentation, timely patch management, multi-factor

authentication, and vendor oversight, each of which is mandated or strongly recommended under PCI DSS and Section 5 of the FTC Act.

35. Slim CD's inadequate security posture enabled threat actors to maintain undetected access to its computer environment from August 17, 2023 through June 15, 2024, siphoning approximately 1.7 million consumers' PCD. The breach has forced Plaintiffs and Class members to: (a) reissue vast numbers of payment cards; (b) reimburse cardholders for fraudulent charges; (c) enhance and prolong fraud-monitoring programs; and (d) expend significant staff time communicating with affected customers and regulatory bodies.

36. The foreseeable and direct result of Slim CD's conduct is tens of millions of dollars in remediation expenses borne by financial institutions. These costs would have been avoided had Slim CD complied with industry standards and exercised reasonable care in protecting PCD

37. The PCI DSS is a comprehensive framework of information security requirements developed by the Payment Card Industry Security Standards Council. These requirements apply to all entities that store, process, or transmit cardholder data, including merchants and service providers like Slim CD. The PCI DSS list is designed to ensure that all companies maintain a secure environment to protect payment card data from unauthorized access and misuse.

38. The 12 requirements of the PCI DSS are:

Build and Maintain a Secure Network

1) Install and maintain Network Security Controls

2) Apply Secure Configurations to All Systems

Protect Account Data

3) Protect Stored Account Data

4) Protect Cardholder Data with Strong Cryptology During Transmission Over Open, Public Networks

Maintain a Vulnerability Management Program

5) Protect All Systems and Networks from Malicious Software

6) Develop and Maintain Secure Systems and Software

Implement Strong Access Control Measures

7) Restrict Access to System Components and Cardholder Data by Business Need to Know

8) Identify Users and Authenticate Access to System Components

9) Restrict Physical Access to Cardholder Data

Regularly Monitor and Test Networks

10) Log and Monitor All Access to System Components and Cardholder Data

11) Test Security of Systems and Networks Regularly

Maintain an Information Security Policy

12) Support Information Security with Organizational Policies and Programs.[5]

39. PCI DSS v4.0.1 imposes heightened obligations on processors such as Slim CD, requiring them to use strong encryption, regularly assess risks, and implement robust authentication and access controls. Slim CD's failure to comply with these obligations, including its failure to encrypt cardholder data, monitor system access, and minimize unnecessary data retention, constitutes a clear violation of PCI DSS.

40. For example, Requirement 3.2 mandates that stored account data be kept to a minimum, retained only as long as necessary for legal or business purposes, and regularly purged.

[5] PCI Security Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 4.0.1* (June 2024), https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf (last visited July 22, 2025).

Slim CD's failure to implement appropriate data retention and deletion protocols contributed directly to the scope of the breach.

41. Requirement 8 of PCI DSS requires multi-factor authentication ("MFA") for all administrative access to systems handling cardholder data. Slim CD failed to implement MFA, thereby enabling unauthorized actors to gain prolonged and unchecked access to sensitive systems.

42. PCI DSS also mandates that covered entities log and monitor access to systems that store or transmit cardholder data, per Requirement 10. Slim CD failed to detect the ongoing intrusion for nearly ten months, demonstrating a lack of basic logging, alerting, and threat detection capabilities.

43. In addition, PCI DSS Requirement 12.8 obligates merchants to ensure that all third-party service providers ("TPSPs") meet applicable security standards and maintain documentation of their compliance. Slim CD failed to adequately oversee or ensure compliance of any vendors or external systems it relied upon for storing or transmitting PCD.

44. These deficiencies collectively reflect Slim CD's systemic failure to follow well-established data security norms and regulatory standards. By disregarding these obligations, Slim CD directly enabled the theft of massive quantities of PCD and exposed financial institutions to widespread, preventable harm.

45. In sum, Slim CD's non-compliance with PCI DSS requirements not only facilitated unauthorized access to sensitive PCD but also violated industry standards to prevent precisely the type of breach that occurred. Slim CD's failure to implement, monitor, and enforce appropriate data security practices has caused substantial financial harm to Plaintiffs and the Class and will continue to do so.

The Data Breach

46. In a notification filed with regulators on dated September 9, 2024, Slim CD disclosed that its systems were compromised, and that an unauthorized actor gained access to its network between August 17, 2023 and June 15, 2024.[6]

47. Slim CD further indicated that while the unauthorized parties had access to Defendant's computer systems, they were able to access and exfiltrate credit card information.[7]

48. As such, Slim's own notice of the Data Breach confirms that the Data Breach was a successful targeted attack, during which cybercriminals were able to steal sensitive PCD.

49. According to the Data Breach notification filed with the State of Maine, approximately 1.7 million persons were affected, drawing from merchants across the U.S. who relied on Slim CD's gateway for processing payments.[8]

Slim CD Collects Extensive Payment Card Data and Knew a Breach was Foreseeable

50. Through its payment-gateway platform, Slim CD processes millions of credit and debit-card transactions each year on behalf of retail, hospitality, and e-commerce merchants across the United States and Canada. To complete each transaction, Slim CD collects and stores highly sensitive PCD, including cardholder names, primary account numbers, expiration dates, and, in many cases, billing addresses.

51. Plaintiffs and Class members, who, as issuing financial institutions, ultimately bear the costs of card fraud, reasonably relied on Slim CD's express and implied representations that it

---

6 *Notice of Data Event*, State of California Department of Justice, https://oag.ca.gov/system/files/Slim%20CD%2C%20Inc.%20-%20Notice%20of%20Data%20Event%20-%20CA_0.pdf (last accessed July 22, 2025).

7 *Id.*

8 *Data Breach Notifications*, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/d23671d5-1c6d-4dce-a78f-2e408daf3545.html (last accessed July 22, 2025).

would maintain PCI DSS-compliant security controls to protect the PCD it processed on their customers' behalf.

52. Despite these assurances, Slim CD failed to implement and enforce reasonable security measures, including (a) strong encryption for cardholder data; (b) MFA for privileged system access; (c) continuous logging and intrusion detection; and (d) routine data-retention purges. These omissions created, and ultimately realized, an unreasonable risk of unauthorized access.

53. The rapidly escalating frequency of payment-card data breaches placed Slim CD on heightened notice that its environment was a prime target for threat actors. Industry reports repeatedly warn payment processors of the severe financial consequences that follow lapses in data security.

54. PCD is a lucrative commodity on underground markets. Stolen card records command premium prices because they can be used to manufacture counterfeit cards, fund large unauthorized purchases, or facilitate account-takeover schemes. Consequently, payment card processors like Slim CD know, or should know, that even a brief lapse in controls can expose millions of dollars in potential fraud losses for issuing banks.

55. Publicly available data further confirms the magnitude of the threat. Thousands of data breaches are publicly disclosed each year, exposing millions of sensitive records; the majority of these incidents involve financially motivated attacks directed at companies who collect, store, and/or process sensitive information such as PCD.

56. Given its role at the nexus of merchant transactions and card-issuer reimbursement, Slim CD was uniquely positioned to appreciate and mitigate the catastrophic downstream impact a breach would have on financial institutions. Yet Slim CD ignored clear regulatory guidance,

failed to invest in adequate safeguards, and left card issuers to shoulder the resulting fraud, card-reissuance, monitoring, and operational costs. Slim CD's conscious disregard of well-known industry standards and regulatory directives constitute negligent, and, under the FTC Act and PCI DSS, negligent *per se*, conduct that directly and proximately caused the injuries suffered by Plaintiffs and the Class.

57. PCD has considerable value and constitute an enticing and well-known target to hackers. Hackers easily can sell such stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[9]

58. "Personal Data is currency in the Information Age and is being traded to the tune of billions of dollars globally – and increasing each year as the more personal data analyzed, categorized and linked."[10]

59. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the Identity Theft Resource Center ("ITRC"), in just the third quarter of 2024, there were 672 reported data breaches in the United States, putting the year on track to see nearly as many breaches as occurred in the record-high year of 2023.[11] More than 241 million individuals' data reportedly were exposed in those breaches (again – just

---

[9] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016, 10:47 AM), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[10] *The Value of Personal and Private Data*, DIGITAL CONTROL ROOM, https://web.archive.org/web/20250424004036/https://www.digitalcontrolroom.com/the-value-of-personal-and-private-data/ (archived April 24, 2025).

[11] *Supply Chain Attacks Roar Back in Q3; Mega-Breaches Drive Increase in Victims*, IDENTITY THEFT RESOURCE CENTER (2024), https://www.idtheftcenter.org/wp-content/uploads/2024/10/ITRC-Q3-2024-Data-Breach-Analysis-1.pdf.

in the third quarter of 2024).[12] The IRTC reported that approximately 549 of the 672 data breaches in the quarter were the result of cyberattacks.[13]

60. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves the customers of Plaintiffs and Class members especially vulnerable to credit card fraud.

61. Cybercriminals can use stolen payment card information to create counterfeit payment cards and make unauthorized charges or withdrawals that can cause consumers to incur significant financial losses. Indeed, the counterfeit payment cards (or the compromised payment card information itself) can be used to purchase high-ticket goods or gift cards that can then be sold for cash all while charging the consumer's original card. Cybercriminals can also sell the stolen payment card information to other cybercriminals on the dark web. In turn, when a payment card is fraudulently used, it can damage the cardholder's credit score, making it difficult to obtain new credit in the future.

62. Following several high-profile data breaches in recent years, including those involving Target, Home Depot, Wendy's Equifax, Wawa, and Ticketmaster, Slim CD was on notice of the very real risk that hackers could exploit vulnerabilities in its data security.

63. Defendant also knew or should have known the importance of safeguarding the PCD with which it was entrusted and of the foreseeable consequences if its data security systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach and the exfiltration of PCD from occurring.

---

12 *Id.*

13 *Id.*

Slim CD Failed to Comply with FTC Guidelines and Industry Standards of Care as to Data Security

64. Slim CD, as a payment gateway and processor entrusted with handling vast quantities of PCD is subject to binding obligations under both federal regulatory frameworks and industry-maintained data security standards.

65. These include compliance with Section 5 of FTC Act, which prohibits unfair or deceptive acts or practices in commerce, and adherence to the PCI DSS.

66. Under Section 5 of the FTC Act, entities engaged in the collection, storage, or processing of sensitive consumer information are required to implement reasonable and appropriate security measures to safeguard that information from unauthorized access or theft.

67. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

68. In 2016, the FTC updated its publication titled Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.[15] The guidelines recommend that businesses implement the following:

a. Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it;"

[14] *See* Federal Trade Commission, *Start with Security: A Guide for Business* (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[15] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

b. Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

d. Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

e. Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.[16]

69. In another publication, the FTC recommended that companies not maintain sensitive information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[17]

70. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act. Indeed, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must

16 *Id.*

17 *See Start with Security: A Guide for Business*, *supra* n. 14.

take to meet their data security obligations. *See, e.g., FTC v. Wyndham Corp.*, 799 F.3d 236, 240 (3d Cir. 2015).

71. Slim CD is also required to comply with PCI DSS, the prevailing industry framework developed to secure payment card transactions and prevent breaches. PCI DSS mandates strict technical and administrative controls for protecting cardholder data, including encryption, logging, access restrictions, and vulnerability assessments.

72. These requirements are not optional. Rather, they serve as baseline obligations that all payment processors must meet to ensure the safety and integrity of the payment ecosystem.

73. By failing to ensure its own compliance, Slim CD violated its duty to protect PCD in accordance with both regulatory and industry requirements.

74. Defendant's failure to employ reasonable and appropriate measures to protect PCD constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

75. Defendant was fully aware of its obligation to safeguard PCD. This awareness stems from industry standards, contractual requirements with third-party vendors, and prior data breaches that highlighted the necessity of robust security measures. Despite this knowledge, Defendant failed to implement appropriate safeguards, prioritizing expediency over security.

76. These failures reflect Slim CD's systemic disregard for established security standards, its regulatory obligations, and the foreseeable consequences of noncompliance. That disregard enabled the unauthorized access and exfiltration of PCD and caused substantial harm to issuing financial institutions.

77. Accordingly, Slim CD's conduct constitutes both common law negligence and negligence *per se*, as Plaintiffs and the Class were within the class of entities the FTC Act and PCI DSS are designed to protect, and the injuries they suffered, fraudulent transactions, card

replacement, increased monitoring, and operational disruptions, are the very harms those frameworks seek to prevent.

FI Plaintiffs Have Been, and Will Continue to Be, Harmed by the Slim CD Data Breach

78. The Data Breach has inflicted substantial and ongoing financial harm on Plaintiff and members of the Class. As financial institutions, Plaintiffs were forced to act immediately to contain fraud, mitigate exposure, and re-secure affected accounts following the unauthorized access and exfiltration of PCD from Slim CD's computer systems.

79. Specifically, Plaintiffs and other financial institutions have had to: (a) cancel and reissue compromised payment cards; (b) investigate and respond to reports of fraudulent activity on those cards; (c) reimburse cardholders for fraudulent transactions; (d) enhance fraud monitoring efforts for affected accounts; (e) provide customer support and notification; and (f) absorb losses stemming from lost interest, transaction fees, and decreased cardholder usage. These actions have imposed significant operational costs and resource burdens.

80. Additionally, debit and credit cards compromised as a result of the breach, including the account number sprinted on the face of the cards, were devalued. The exposure of this information undermines consumer trust in the affected cards, requiring institutions to replace cards even in the absence of confirmed fraud to maintain customer confidence.

81. These losses are not speculative. Beginning in or about August 2024, major card networks including Visa and Mastercard began issuing CAMS alerts to financial institutions, designating Slim CD as the source of a significant payment card breach. The CAMS alerts indicated an exposure window of compromised cards starting on October 21, 2023 and ending on July 15, 2024.

82. These alerts confirmed that card data, including cardholder names, PANs, expiration dates, and potentially other data, had been compromised. These alerts enable card-issuing institutions to identify affected accounts and initiate appropriate mitigation procedures.

83. By October 24, 2025, Plaintiffs had each received at least one alert referencing Slim CD. Each alert required immediate action to review, assess, and mitigate potential exposure, diverting institutional resources and resulting in direct financial loss. Plaintiffs received additional alerts referencing Slim CD as recently as June 2025.

84. In total, Plaintiffs and Class members have suffered and will continue to suffer damages due to Slim CD's failure to safeguard sensitive PCD, including the costs of card replacement, reimbursement for fraud, lost revenue, increased administrative costs, and harm to institutional reputation. These harms are ongoing and expected to persist as stolen card data circulates in criminal marketplaces.

CLASS ACTION ALLEGATIONS

85. Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of the following nationwide class ("Nationwide Class" or the "Class"):

Nationwide Class

> All Financial Institutions in the United States (including its Territories and the District of Columbia) whose consumers' PCD was exposed as a result of the Slim CD Data Breach announced on or about September 2024.

86. Excluded from the Class are Defendant Slim CD, any entity in which Slim CD has a controlling interest, Slim CD's officers and directors, the Court and its staff, and any members of their immediate families.

87. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when they move

for class certification as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

Rule 23(a)

88. This action may properly be maintained as a class action and satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

89. **Numerosity.** The members of the Class are so numerous and geographically dispersed that joinder would be impracticable. The number of Class members exceeds 100. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach.

90. **Commonality and Predominance.** There are common questions of law and fact that predominate over questions affecting only individual Class members. These common legal and factual questions include, but are not limited to:

a. whether Defendant owed a duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and members of the Class when obtaining, storing, using, and managing PCD, including taking action to safeguard such data;

b. whether Defendant actively mishandled PCD and implemented and maintained data security measures that it knew or should have known were unreasonable and inadequate to protect PCD;

c. whether Defendant negligently allowed PCD to be accessed, used, or disclosed by third parties;

d. whether Plaintiffs and members of the Class justifiably relied on representations made by Slim CD as to its data security practices and the integrity and accuracy of PCD Slim CD provided;

e. whether Plaintiffs and members of the Class justifiably relied on representations made by Slim CD that it would oversee and protect PCD given to third parties and ensure that such entities maintained adequate data security practices and the integrity and accuracy of the PCD Slim CD provided;

f. whether Slim CD intended that Plaintiffs and members of the Class would rely on Slim CD's representations as to its data security practices and the integrity and accuracy of information Slim CD provided;

g. whether Slim CD failed to adequately notify Plaintiffs and members of the Class that its data systems were breached;

h. whether Plaintiffs and members of the Class were injured and suffered damages and ascertainable losses;

i. whether Slim CD actions and inactions failed to provide reasonable security proximately caused the injuries suffered by Plaintiffs and members of the Class;

j. whether Plaintiffs and members of the Class are entitled to damages and, if so, the measure of such damages; and

k. whether Plaintiffs and members of the Class are entitled to injunctive, equitable, declaratory and/or other relief, and if so, the nature of such relief.

91. **Typicality.** Plaintiffs' claims are typical of the claims of the absent class members and have a common origin and basis. Plaintiffs and absent Class members are all financial institutions injured by Slim CD's Data Breach. Plaintiffs' claims arise from the same practices and course of conduct giving rise to the claims of the absent Class members and are based on the same legal theories, namely the Slim CD Data Breach. If prosecuted individually, the claims of each Class member would necessarily rely upon the same material facts and legal theories and seek the same relief. Plaintiffs' claims arise from the same practices and course of conduct that give rise to the other Class members' claims and are based on the same legal theories.

92. **Adequacy.** Plaintiffs will fully and adequately assert and protect the interests of the absent Class members and have retained Class counsel who are experienced and qualified in prosecuting class action cases similar to this one. Neither Plaintiffs nor their attorneys have any interests contrary to or conflicting with the interests of absent Class members.

Rule 23(b)(3)

93. The questions of law and fact common to all Class members predominate over any questions affecting only individual class members.

94. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class members' claims is economically infeasible and procedurally impracticable. Class members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class members to litigate their claims where it would otherwise be too expensive or

inefficient to do so. Plaintiffs know of no difficulties in managing this action that would preclude its maintenance as a class action.

Rule 23(b)(2)

95. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Slim CD. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

96. Contact information for each Class member, including mailing addresses, is readily available, facilitating notice of the pendency of this action.

LEGAL CLAIMS

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

97. Plaintiffs repeat and reallege the allegations contained in paragraphs 1-96 above as if fully set forth herein.

98. Defendant owes a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and members of the Class when obtaining, storing, using, selling, and managing PCD, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class of any breach in a timely manner so that appropriate action can be taken to minimize or avoid losses. This duty arises from several sources (described below) and is independent of any duty as a result of any contractual obligations.

99. Slim CD has a common law duty to prevent the foreseeable risk of harm to others, including the Plaintiffs and the Class. It was certainly foreseeable to Slim CD that injury would result from a failure to use reasonable measures to protect PCD and to provide timely notice that a breach was detected. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal PCD belonging to hundreds of thousands of individuals whose PCD was processed though Slim CD gateway; thieves would use PCD to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud by cancelling and reissuing the compromised cards and reimbursing their customers for fraud losses; and that the resulting financial losses would be immense.

100. Slim CD assumed the duty to use reasonable security measures as a result of its conduct when processing the PCD of Plaintiffs' and the Class's customers.

101. In addition to its general duty to exercise reasonable care, Slim CD also had a duty of care as a result of the special relationship that existed between Slim CD and the Plaintiffs and members of the Class. The special relationship arose because financial institutions entrusted Slim CD with PCD. Only Slim CD was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from the Data Breach

102. Defendant's duty to use reasonable data security measures also arose under Section 5 of FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PCD by businesses such as Slim CD. The FTC's publications and data security breach orders described above further form the basis of Slim CD's duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty on the part of Defendant.

Defendant's lax and deficient data security measures, and failure to promptly notify Plaintiffs and the Class of the Data Breach constitute unfair practices in violation of the FTC Act.

103. Defendant's duty to use reasonable care in protecting PCD arose not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards, specifically including duties under PCI DSS.

104. Defendant breached its common law, statutory, and other duties and thus, was negligent by failing to use reasonable measures to protect Plaintiffs' PCD from the hackers who perpetrated the Data Breach and by failing to provide timely notice of the breach. Upon information and belief, the specific negligent acts and omissions committed by Defendant include, but are not limited to, some, or all, of the following:

a. failure to protect, store and delete PCD after the time period necessary to authorize the transaction;

b. failure to implement systems to protect against malware;

c. failure to comply with industry standards for multi-factor authentication and security of PCD;

d. failure to maintain adequate firewalls;

e. failure to track and monitor access to its network and PCD;

f. failure to limit access to PCD to those with a valid purpose;

g. failure to encrypt PCD;

h. failure to adequately staff and fund its data security operations;

i. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations;

j. failure to recognize red flags signaling that Defendant's systems were inadequate and that, as a result, the potential for a massive data breach was increasingly likely;

k. failure to recognize that cybercriminals had infiltrated systems containing PCD and were stealing PCD while the Data Breach was taking place; and

l. failure to disclose the Data Breach in a timely manner.

105. In connection with the conduct described above, Defendant acted wantonly, recklessly, and with complete disregard for the consequences.

106. As a direct and proximate result of Defendant's negligence, Plaintiffs and members of the Class have suffered, and continue to suffer, injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. Plaintiffs and the Class also lost interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

107. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

108. Plaintiffs repeat and reallege the allegations contained in paragraphs 1-96 above as if fully set forth herein.

109. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Slim CD, of failing to use reasonable measures to protect PCD. The FTC publications and orders described above also form part of the basis of Defendant's duty.

110. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiffs' and the Class's PCD and failing to comply with applicable industry standards, including PCI DSS, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PCD it obtained (PCD related to at least 1.7 million individuals) and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers, Plaintiffs and the Class.

111. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

112. Plaintiffs and members of the Class are within the class of persons that Section 5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for directly reimbursing consumers for fraud losses. Moreover, many of the Class members are credit unions, which are organized as cooperatives whose members are consumers.

113. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by the Plaintiffs and the Class.

114. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers. They also lost interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

115. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

116. Plaintiffs repeat and reallege the allegations contained in Paragraphs 1-96 and 97-115 above as if fully set forth herein.

117. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious, and which violate the terms of the federal and state statutes described herein.

118. An actual controversy has arisen in the wake of the Data Breach regarding its common law and other duties to reasonably safeguard PCD. Plaintiffs allege that Defendant's data security measures were inadequate and remain inadequate. Plaintiffs anticipate that Defendant will deny these allegations. Furthermore, Plaintiffs continue to suffer injury as additional compromised

payment cards are identified and need to be reissued and as additional fraudulent charges are made on payment cards they issued to their customers whose PCD was processed by Slim CD.

119. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure the PCD its collects, stores, and processes and to notify financial institutions of a data breach under the common law, Section 5 of the FTC Act, PCI DSS standards, its commitments, and various state statutes;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PCD; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs and the Class harm.

120. The Court also should issue corresponding injunctive relief requiring Defendant to employ adequate security protocols, consistent with industry standards, to protect PCD. Specifically, this injunction should, among other things, direct Defendant to:

a. utilize industry standard encryption to require multi-factor authentication for Defendant's computer systems;

b. require that PCD be encrypted at all other times;

c. require that Defendant only maintain PCD for a limited time where it has an ongoing need to use such data;

d. require Defendant to delete all historical PCD that it possesses;

e. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

f. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

g. regularly test its systems for security vulnerabilities, consistent with industry standards;

h. comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information; and

i. install all upgrades recommended by manufacturers of security software and firewalls used by Defendant.

121. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Slim CD. The risk of another such breach is real, immediate, and substantial. If another breach at Slim CD occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for out-of-pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable and reputational damage.

122. The hardship to Plaintiffs and the Class, if an injunction is not issued, exceeds the hardship to Defendant, if an injunction is issued. Among other things, if another massive data breach occurs at Slim CD, Plaintiffs and members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable data security measures is relatively minimal, and Defendant have a pre-existing legal obligation to employ such measures.

123. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Slim CD, thus eliminating the injuries that would result to Plaintiffs, the Class, and the millions of consumers whose confidential information would be compromised.

FOURTH CLAIM FOR RELIEF
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

124. Plaintiffs restate and reallege the allegations contained in paragraphs 1-96 above as if fully set forth herein.

125. Plaintiffs and Class members conferred a monetary benefit on Defendant by directly and/or indirectly providing them with their valuable PCD.

126. Defendant knew that Plaintiffs and Class members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PCD entrusted to it.

127. Defendant profited from Plaintiffs' and Class members' PCD and use of Plaintiffs' and Class members' PCD for business purposes.

128. Defendant failed to secure Plaintiffs' and Class members' PCD and, therefore, did not fully compensate Plaintiffs or Class members for the value that their PCD provided.

129. Defendant acquired Plaintiffs' and the Class's PCD through inequitable record retention as Defendant failed to disclose the inadequate data security practices previously alleged.

130. If Plaintiffs and Class members had known Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PCD, they would not have agreed to the entrustment of their PCD to Defendant.

131. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class members conferred upon Defendant.

132. Plaintiffs and Class members are without an adequate remedy at law

133. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered injuries, including those identified above.

134. Plaintiffs and Class members are entitled to restitution and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct, as well as return of their sensitive PCD and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class members may seek restitution or compensation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request that the Court:

A. Certify the Class and appoint Plaintiffs and Plaintiffs' counsel to represent the Class;

B. Enter a monetary judgment in favor of Plaintiffs and the Class to compensate them for the injuries they have suffered and will continue to suffer, together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

C. Enter a declaratory judgment as described herein and corresponding injunctive relief requiring Defendant to employ adequate data security protocols consistent with industry standards to protect PCD;

D. Grant the injunctive relief requested herein;

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and

F. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all claims so triable.

Date: July 22, 2025

Respectfully submitted,

/s/ Gary F. Lynch
Gary F. Lynch (Pa. ID No. 56887)
Patrick D. Donathen (Pa. ID No. 330416)
LYNCH CARPENTER LLP
1133 Penn Avenue, Fifth Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com
patrick@lcllp.com

Joseph P. Guglielmo (*pro hac vice* forthcoming)
Andrew Stanko (*pro hac vice* forthcoming)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 24th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
astanko@scott-scott.com

Attorneys for Plaintiffs