IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOHN DOE 1, individually and on behalf of all others similarly situated, Plaintiff, v. STRETTO, INC., Defendant.	Case No.: 1:26-cv-3477 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff John Doe 1[1] ("Plaintiff" or "John Doe 1"), individually and on behalf of all others similarly situated, alleges the following against Defendant Stretto, Inc. ("Stretto" or "Defendant"). Plaintiff's allegations are based on personal knowledge as to himself, on the public record in three bankruptcy cases relating to cryptocurrency companies, on notices issued by Stretto and the affected estates, on information obtained from affected creditors, and on the continuing investigation of counsel.

[1] In light of the serious financial harm Plaintiff has suffered due to the unlawful exposure of his highly sensitive personal and financial information, as well as his continued exposure to potential additional harm, it is appropriate to use a pseudonym to reference Plaintiff in this publicly filed complaint, as further explained in Plaintiff's motion to proceed under a pseudonym, which Plaintiff has filed contemporaneously herewith. *See, e.g.*, *Sealed Plaintiff v. Sealed Defendant*, 537 F.3d 185, 189 (2d Cir. 2008) (establishing "the standard governing the use of pseudonyms in civil litigation in our Circuit"); *Doe v. DNA Diagnostics Ctr. LLC*, 1:25-cv-2878-GHW, 2025 WL 1725449, at *1 (S.D.N.Y. June 18, 2025) (allowing plaintiff to proceed pseudonymously).

NATURE OF THE ACTION

1. This case arises from Stretto's April 2024 security incident ("Data Breach") and from Stretto's ensuing failure to administer creditor communications and distributions in a manner reasonably calculated to protect known cryptocurrency creditors. Stretto was entrusted with personally identifiable information ("PII") of creditors in three bankruptcy cases: *In re Celsius Network LLC*, No. 22-10964 (MG) (Bankr. S.D.N.Y.) ("*Celsius*"), *In re Voyager Digital Holdings, Inc.*, No. 22-10943 (MEW) (Bankr. S.D.N.Y.) ("*Voyager*"), and *In re Prime Core Technologies Inc.*, No. 23-11161 (JKS) (Bankr. D. Del.) ("*Prime Core*"). Those cases involved hundreds of thousands of cryptocurrency creditors whose identifying information was protected by the Bankruptcy Court because of the obvious risk that criminals would use that information to target crypto holders.

2. On or about April 17, 2024, Stretto discovered suspicious activity in a Stretto employee account. The incident was not a theoretical privacy lapse. The threat actor accessed Stretto's CORE claims-administration environment and exfiltrated data held by Stretto in connection with bankruptcy matters. In *Celsius*, at least 104,000 creditors had PII, as that term is defined in 11 U.S.C. § 101(41A), accessed or exfiltrated. In *Prime Core*, Stretto later reported that approximately 142,200 creditors were impacted and that exposed fields included names, addresses, phone numbers, fax numbers, email addresses, claim amounts, schedule amounts, and/or voting amounts, with Social Security or taxpayer identification numbers present for 23 creditors. And In *Voyager*, Stretto estimated 381,137 creditors had PII compromised similarly by the Data Breach.

3. Stretto and its counsel tried to minimize the breach by distinguishing "contact information" from more "sensitive" data. Judge Martin Glenn rejected that framing at the May 14,

2024 Celsius hearing.[2] The Bankruptcy Code expressly defines PII to include a creditor's first initial and last name, physical address, email address, telephone number, Social Security number, and credit-card account number. Judge Glenn therefore pressed Stretto's counsel who acknowledged that approximately 104,000 Celsius creditors had PII wrongfully obtained. 11 U.S.C. § 101(41A). Judge Glenn emphasized that names, home addresses, email addresses, and phone numbers are "all really important information" and "all PII under the Bankruptcy Code."[3]

4. The Data Breach was particularly dangerous because the contact information of cryptocurrency creditors is not ordinary contact information. A name, email address, telephone number, mailing address—particularly when exfiltrated in conjunction with a bankruptcy claim amount—not only identify a person as a cryptocurrency creditor, but also reveal that the creditor may be expecting a distribution, and can enable targeted phishing, account takeover, social engineering, SIM-swap attempts, wallet-drainer lures, extortion, and physical mail scams.

5. The Stretto and the Celsius estates knew this. That is why creditor addresses, email addresses, and telephone numbers were sealed in the bankruptcy proceedings. That is also why Stretto's failure to protect, notify, and safely administer post-breach distributions caused concrete harm.

6. Yet, after the Data Breach, Stretto failed to promptly notify affected creditors. At the May 14, 2024 hearing, Judge Glenn stated that the "radio silence" from April 17 to May 7 was "mindboggling."[4] Stretto only began notifying certain creditors on May 7, 2024, the day on which Judge Glenn had already expressed grave concern at an earlier hearing that affected creditors had

[2] *In re Celsius Network LLC*, No. 22-10964 (MG), ECF No. 4892, at 12–13 (Bankr. S.D.N.Y. May 17, 2024).
[3] *Id.* at 24, 41.
[4] *Id.* at 9.

not yet been contacted. Stretto also failed to promptly notify all presiding judges in the affected bankruptcy cases until Judge Glenn ordered Stretto to do so.

7. The Data Breach immediately translated into creditor-facing harm. Voyager reported that it began receiving reports of phishing attempts targeting Voyager creditors on May 6, 2024, before Stretto had provided Voyager the promised summary report or substantive answers to Voyager's questions. Voyager was forced to warn creditors that all future distributions would be by check, that Voyager would not ask creditors to connect wallets, and that creditors should report suspicious letters, emails, text messages, or phone calls imitating Voyager. A representative Voyager-themed postal phishing letter later circulated to creditors purporting to offer an "additional total value return," instructing the recipient to use an ERC-20 wallet, and directing the recipient to a fraudulent domain, "withdrawal-investvoyager.com."

8. The *Celsius* distribution process likewise was disrupted. The *Celsius* Plan Administrator's First Status Report states that the Data Breach required pausing distributions for approximately one month and that, following the Stretto incident, all unclaimed PayPal and Venmo claim codes were invalidated and reissued. The report also identifies widespread email deliverability issues, creditor confusion, and tens of thousands of creditors who had not yet received distributions. These were not abstract administrative inconveniences. They were foreseeable consequences of contaminating the primary email channel used to deliver rights-critical and distribution-critical communications to a crypto creditor population already facing sophisticated impersonation attacks.

9. John Doe 1 is a Celsius creditor. After the Data Breach, he was inundated with spam, spoofed estate and Stretto-branded communications, phone calls, suspicious postal solicitations, and sophisticated social-engineering attempts. Threat actors attempted to take over

John Doe 1's email and financial accounts. Out of an abundance of caution, John Doe 1 attempted to contact the estate, Stretto, and/or distribution support by telephone and email, but the post-Data Breach support structure made it practically impossible to obtain a reliable response or to authenticate distribution communications. John Doe 1's email inbox was flooded with lookalike and spoofed Stretto/Celsius communications, and he did not receive an official postal backstop that would allow him to verify rights-critical distribution instructions through a safe and secure channel.

10. John Doe 1 has not timely received all his distributions after the Data Breach. He has suffered concrete injuries including loss of control of his PII, actual targeted misuse of his PII, attempted account takeover, out-of-pocket security-hardening expenses, time spent investigating and mitigating the Data Breach, loss of productivity, lost use and time value of delayed Celsius distributions, and anxiety and distress caused by the exposure of identifying information that ties him to a large cryptocurrency claim.

11. Plaintiff John Doe 1 brings this action to recover damages for Stretto's Data Breach and its post-breach administration failure, and to obtain narrow injunctive relief that restores safe distribution communications at Stretto's expense so that estate distributions to creditors are not reduced.

PARTIES

12. Plaintiff John Doe 1 is a natural person and Celsius creditor residing in Hennepin County, Minnesota. He held a large claim in the Celsius bankruptcy. He has experienced delays receiving distributions because phishing intensified due to the Data Breach. He uses a pseudonym because disclosure of his name in connection with this complaint would amplify the very crypto-targeting risk at issue.

13. Defendant Stretto, Inc. is a Delaware corporation with its principal place of business in Irvine, California. Stretto provides claims, noticing, solicitation, distribution, restructuring-administration, and related technology services in bankruptcy cases. Stretto maintains a New York presence and, on information and belief, performed material work for the Celsius, Voyager, and Prime Core bankruptcy cases from, through, or directed to its New York office, including work connected to claims administration, noticing, creditor communications, distribution administration, and post-breach response.

14. Stretto was appointed to perform claims and noticing functions in bankruptcy cases pending in this District, including *Celsius*, *Voyager*, and *Prime Core*. Stretto's retention required court approval, and Stretto functioned in place of the Clerk's Office for claims and noticing functions. It thereby accepted duties to protect Bankruptcy Code PII, to preserve the integrity of official creditor communications, and to administer claims and distributions without exposing creditors to reasonably foreseeable harm.

JURISDICTION

15. This Court has subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action under Rule 23 of the Federal Rules of Civil Procedure, the proposed class includes more than 100 members, at least one class member is a citizen of a state different from Defendant, and the amount in controversy exceeds $5,000,000 exclusive of interest and costs.

16. The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over related state-law claims that form part of the same case or controversy.

17. This Court has personal jurisdiction over Stretto because Stretto maintained and maintains continuous contacts with New York, including a New York office; because Stretto was

retained to perform claims and noticing work in bankruptcy cases pending in the Southern District of New York; because Stretto appeared, through counsel and representatives, in this District in connection with the April 2024 Data Breach; and because the claims asserted here arise from Stretto's New York-directed and New York-connected conduct. Plaintiff's claims arise out of and relate to these substantial contacts.

18. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in this District, including the *Celsius* and *Voyager* bankruptcy cases, Stretto's court-approved claims-agent work, Stretto's reporting to the Bankruptcy Court, and the distribution-administration failures that harmed Plaintiff and the class. Venue is also appropriate because Stretto is subject to personal jurisdiction in this District and maintains a New York office.

19. Plaintiff challenges Stretto's security configuration, data minimization, employee-account controls, breach scoping, notification timing, post-breach channel design, failure to provide postal backstops, failure to provide reliable human support, and failure to remediate delayed distributions. No court order required Stretto to use inadequate security, delay notice until completion of a forensic report, rely on contaminated email channels, omit postal backstops, or provide ineffective support to affected creditors.

BACKGROUND

A. Relevant Bankruptcy Code Definitions and Concepts.

20. For a full understanding of Plaintiff's claims, several terms and concepts related to cryptocurrency, the Data Breach, the Celsius bankruptcy distribution process, and the social engineering attacks against Plaintiff warrant further explication.

a. **Bankruptcy Code PII**: The Bankruptcy Code defines "personally identifiable information" broadly. Under 11 U.S.C. § 101(41A), PII includes, when provided by an individual to a debtor in connection with obtaining a personal, family, or household product or service, the individual's first name or initial and last name, physical address, email address, telephone number, Social Security number, or credit-card account number. It also includes other information identified in connection with those data elements that would result in contacting or identifying the individual physically or electronically.

b. **Claims and noticing agents**: Claims and noticing agents appointed under 28 U.S.C. § 156(c) perform clerk-type functions in bankruptcy cases, including maintaining creditor matrices, servicing notices, receiving and maintaining proofs of claim, and maintaining claims registers. Because they handle court-protected creditor PII and perform official notice functions, they must employ reasonable safeguards and administer notice in a manner reasonably calculated to apprise known creditors of rights-affecting events.

c. **Crypto creditor PII**: For cryptocurrency creditors, the combination of name, email address, phone number, physical address, claim amount, distribution-agent assignment, account status, and bankruptcy-claim context is uniquely dangerous. It lets criminals identify who owns or is expecting cryptocurrency or cash distributions, prioritize high-value targets, impersonate estate professionals, craft domain and brand-specific lures, attempt exchange-account takeovers, and contact victims through email, phone, text, and physical mail.

d. **Distribution-critical communications**: In Celsius, distribution communications included claim codes, instructions to use PayPal/Venmo, Coinbase, wire transfer, check, Hyperwallet, and other payment mechanisms, and instructions to cure KYC or account-matching issues. When the email channel is contaminated by impersonation, distribution-critical

communications require backstops, including reliable postal mail, visible authenticity cues, and responsive human support.

B. Stretto Was Entrusted with Sealed and Protected Cryptocurrency Creditor PII.

21. Celsius filed its chapter 11 case in this District in July 2022. The Celsius case involved an unusually large, geographically dispersed creditor body. By August 2024, the Plan Administrator reported that distributions under the Plan involved approximately 375,000 creditors in more than 165 countries.

22. Voyager also filed its chapter 11 case in this District, and Stretto served as claims and noticing agent in those cases. Like Celsius, Voyager involved cryptocurrency creditors and distributions, making creditor identity and contact information valuable to threat actors.

23. From the outset of the Celsius case, the Bankruptcy Court recognized that disclosure of creditor addresses, email addresses, and phone numbers would expose Celsius creditors to phishing, social engineering, and other unlawful injury. Judge Glenn explained at the May 14, 2024 hearing that he had granted sealing as to "addresses, email addresses, phone numbers" because of those risks.[5]

24. The same risk was repeatedly confirmed in public filings, creditor reports, and post-breach events. Scammers targeted Celsius, Voyager, and Prime Core creditors with emails, phone calls, lookalike domains, and postal mail. These attacks sought to exploit creditors' expectations of distributions and confusion regarding claims, claim codes, exchange accounts, and wallet instructions.

[5] *In re Celsius Network LLC*, No. 22-10964 (MG), ECF No. 4892, at 24 (Bankr. S.D.N.Y. May 17, 2024).

25. Stretto's position gave it access to precisely the data criminals needed to execute those attacks: names, physical addresses, email addresses, telephone numbers, claim submissions, claim amounts or amount-bearing records, distribution status information, and other claim-administration data.

C. The April 2024 Stretto Data Breach Exposed Bankruptcy PII in Multiple Cases.

26. On April 17, 2024, Stretto information-technology personnel were alerted to suspicious activity involving a Stretto employee account. Stretto later told the Bankruptcy Court that the impacted employee had fallen victim to a "smishing" attack.

27. Stretto's counsel represented at the May 14, 2024 Celsius hearing that Stretto accounts used passwords and multi-factor authentication and that employees were trained to recognize such attacks. Those representations underscore that Stretto knew the attack vector was foreseeable and that employee-account compromise was a material risk.

28. The threat actor accessed Stretto's CORE claims-administration software. Stretto's confidential memorandum, as discussed on the public record at the May 14 hearing, stated that the threat actor "accessed and exfiltrated certain data held by Stretto in connection with the Celsius bankruptcy matter."

29. The threat actor also accessed or exfiltrated information associated with other bankruptcy matters. At the May 14 hearing, Stretto's counsel acknowledged three other affected bankruptcy cases in addition to Celsius. Judge Glenn ordered Stretto to notify the presiding judges, the United States Trustee, and the Chief Deputy Clerk by noon the next day regarding the affected cases and the PII compromised.

30. The affected Celsius population was substantial. Stretto's counsel eventually acknowledged that approximately 104,000 Celsius creditors had PII, as defined by the Bankruptcy

Code, accessed or exfiltrated. A subset of 33 creditors had Social Security numbers or taxpayer identification numbers in the impacted data, but Judge Glenn emphasized that the broader set of names, addresses, emails, and phone numbers was PII and important.

31. The Prime Core notice filed in the District of Delaware stated that Stretto determined that information related to approximately 142,200 creditors was impacted. The impacted fields varied but included names, addresses, phone numbers, fax numbers, email addresses, claim amounts, schedule amounts, and/or voting amounts. For 23 creditors, a Social Security number or taxpayer identification number was also present.

32. The Voyager notice filed in this District stated that Voyager learned from Stretto on April 23, 2024 that Stretto had discovered a data-security incident involving Stretto systems that occurred on or about April 17, 2024. Stretto told Voyager that the affected CORE system stored documents containing names, mailing addresses, and email addresses of Voyager creditors. Voyager asked Stretto questions on April 29 and April 30, 2024, but reported on May 15 that, despite multiple requests, it had not received the promised summary report or substantive responses.

33. By May 6, 2024, Voyager had begun receiving reports of phishing attempts targeting Voyager creditors. On May 9, 2024, after Stretto still had not provided substantive answers, Voyager sent its own email to creditors warning them to be diligent and explaining that Voyager would not make further in-kind distributions and would never ask creditors to connect a wallet.

34. Voyager's May 15, 2024 notice warned creditors that suspicious communications may include "letters, emails, text messages, or phone calls imitating Voyager" and promising additional in-kind withdrawals. This warning was prescient. A representative Voyager-themed

postal phishing letter purported to be signed by Voyager's former chief executive officer, referenced an "Additional Total Value Return for Priority Customers," directed the recipient to an ERC-20 wallet, and instructed the recipient to visit "withdrawal-investvoyager.com."

D. Judge Glenn Made Clear that Stretto's "Contract Information" Framing Was Wrong.

35. At the May 14, 2024 Celsius hearing, Judge Glenn focused on the distinction Stretto attempted to draw between Social Security numbers and the broader creditor contact information. Judge Glenn read the Bankruptcy Code's definition of PII on the record, and emphasized that PII includes first initial and last name, physical address, email address, telephone number, Social Security number, and credit-card account number.

36. When Judge Glenn asked how many Celsius account holders had PII obtained under the Bankruptcy Code definition, Stretto's counsel answered that the number was approximately 104,000.

37. Judge Glenn stated that the information Stretto tried to describe as less sensitive—names, mailing addresses, email addresses, and phone numbers—was important and was PII under the Bankruptcy Code. He explained: "That's a big deal to me," and emphasized that this was information he had ordered not be disclosed.

38. Judge Glenn further stated that in Celsius, when people improperly obtained email and home addresses, there had already been threats, attempts to gain access to accounts, and attempts to access distributions. He explained that identifying information such as addresses, phone numbers, and email addresses was "very serious."

39. Judge Glenn also criticized Stretto's delayed creditor notification. Stretto learned of the incident on April 17, 2024, but did not begin notifying affected Celsius creditors until May

7, 2024. Judge Glenn described the absence of creditor notice between April 17 and May 7 as "mindboggling."

40. Judge Glenn questioned whether Stretto had a written policy for promptly notifying account holders whose PII was improperly accessed. Stretto's counsel did not know. Judge Glenn directed Stretto to provide any such policies to the Court and the United States Trustee.

41. Judge Glenn also made clear that Stretto's obligations ran to the Court, not only to debtor's counsel. He explained that claims agents are "standing in place of the Clerk's Office" and that claims agents appointed by the Court must timely notify the Court when PII protected in bankruptcy cases is compromised.

E. The Data Breach Created Foreseeable Crypto-Specific Threats.

42. The April 2024 Data Breach did not expose ordinary consumer contact lists. It exposed names, contact information, and claim-related information associated with known cryptocurrency bankruptcy creditors who were expecting distributions or post-confirmation communications.

43. Threat actors targeting crypto holders use leaked creditor datasets to identify and prioritize victims. They can combine bankruptcy claim data, public schedules, public crypto-transaction information, data broker information, email addresses, telephone numbers, physical addresses, and exchange-account clues to craft lures that appear credible. They can then contact victims by email, phone, text, and mail and impersonate a bankruptcy estate, claims agent, distribution agent, exchange, wallet provider, or court.

44. These threats are particularly acute where, as in *Celsius*, the bankruptcy record had already disclosed extensive creditor names or transaction information while sealing addresses,

emails, and phone numbers. Cybercriminals could connect public bankruptcy data to real-world addresses, inboxes, and telephone numbers.

45. The foreseeable attack paths include Stretto/Celsius-branded emails, lookalike domains, fraudulent "withdrawal" or "claim code" pages, fake Coinbase support calls, fake PayPal/Venmo code assistance, SIM-swap and account-recovery attempts, fake postal notices, and social-engineering calls referencing real bankruptcy details.

46. Stretto and the estates knew these risks. Voyager's notice warned creditors not to connect wallets, not to trust communications from domains other than @investvoyager.com, and to report suspicious letters, emails, text messages, or phone calls. The Celsius Plan Administrator's later phishing recommendations similarly warned creditors never to connect a crypto wallet anywhere, even if a website looked like a Celsius or Stretto site.

F. Stretto's Delayed Notice and Inadequate Post-Data Breach Administration Magnified the Harm.

47. Stretto waited until the forensic investigation concluded before providing broad creditor notice, even though the risk to creditors was immediate and obvious. A prompt warning could have told creditors that Stretto/Celsius/Voyager-themed communications were unsafe, that claims-agent communications might be spoofed, and that creditors should not click links, connect wallets, provide credentials, or rely solely on email.

48. Stretto's delay left creditors exposed during the critical period when threat actors could use freshly compromised data to launch impersonation campaigns. By May 6, before Stretto had provided Voyager answers and before broad mailed notice, Voyager was already receiving phishing reports.

49. Stretto also failed to implement a communication program reasonably calculated to reach affected creditors under the circumstances. Once Stretto knew that creditor email addresses

had been compromised and that email impersonation was occurring, it was unreasonable to rely primarily on email and portal workflows without postal backstops, verified telephone support, prominent phishing exemplars, and individualized distribution-status assistance.

50. The Celsius Plan Administrator's First Status Report confirms that the Data Breach disrupted distributions. The report states that external factors, including "a data breach," required pausing distributions for approximately one month. It also states that following the Stretto incident, all unclaimed PayPal/Venmo claim codes were invalidated and reissued, and that Stretto was directed to resend claim codes to creditors who did not receive them initially because of email issues such as bounce-backs and spam filtering.

51. The report further confirms that post-effective-date communications were plagued by email deliverability issues. The Post-Effective Date Debtors reported that some email services were flagging estate and Stretto communications as spam or not delivering them at all. These delivery failures occurred against the backdrop of spoofed Stretto and estate communications flooding creditors' inboxes.

52. The distribution impact was substantial. As of August 2024, approximately 121,000 eligible Celsius creditors had not yet successfully claimed a distribution. PayPal had approximately 49,909 creditors with active claims, including 1,030 creditors with distributions greater than $10,000 totaling approximately $41.08 million. Coinbase had approximately 55,607 creditors in process, including 970 creditors with distributions greater than $10,000 totaling approximately $59.61 million.

53. High-value creditors like John Doe 1 suffered especially concrete harm from distribution delay because of time-value loss, market exposure, and lost ability to use, sell, reinvest, secure, or otherwise manage distributed assets scale with claim size.

G. John Doe 1 and the Class Have Been Injured by the Data Breach.

54. John Doe 1 is a Celsius creditor with a six-figure claim. Before Stretto's April 2024 Breach, he received his first distribution. His ability to receive that distribution demonstrates that, before the Breach and the resulting communications breakdown, he was a reachable creditor who could receive and act on official distribution communications.

55. After the Breach, John Doe 1's threat environment changed materially. He began receiving a flood of spam and lookalike communications tied to Celsius creditor distributions, wallet withdrawals, and exchange-account security. He received or was targeted by suspicious postal communications, phone calls, and emails designed to exploit his status as a crypto bankruptcy creditor expecting distributions.

56. The communications were not generic spam. They were estate- and claims-process-themed social-engineering attempts that exploited facts made valuable by the Stretto Data Breach: Plaintiff's name, email address, phone number, mailing address, status as a crypto creditor, and large claim size. The attempts included calls and messages purporting to assist with distributions, account security, or withdrawal processes.

57. Threat actors attempted to take over John Doe 1's crypto exchange account. Coinbase is a Celsius distribution agent, and Celsius distributions required creditors to open matching Coinbase accounts and pass KYC. A Coinbase account takeover attempt directed at a high-value Celsius creditor after the breach is exactly the type of harm Stretto and the estates warned could follow from exposing crypto creditor PII.

58. John Doe 1 did not merely face a speculative future risk. He experienced actual targeted misuse of his PII and attempted account compromise. His inbox, telephone, and physical-

mail channels were contaminated by impersonation attempts, making it unsafe to rely on the ordinary email-based distribution workflow without additional authentication and support.

59. Out of an abundance of caution, John Doe 1 attempted to contact the estate, Stretto, and/or creditor support to verify the status of his distributions and determine which communications were legitimate. He called and emailed but received no meaningful response. The support measures implemented after the Breach made it practically impossible for him to obtain reliable, individualized assistance.

60. John Doe 1 expected an official postal backstop once the email channel became unsafe. Instead, while his email inbox was flooded with lookalike and spoofed Stretto/Celsius communications and while suspicious postal solicitations circulated, he did not receive an official postal notice sufficient to authenticate distribution steps or resolve his account status.

61. To mitigate the Breach and targeted attacks, John Doe 1 was forced to harden his security. His mitigation included opening and migrating to new accounts, replacing or changing credentials, implementing stronger multi-factor authentication, monitoring exchange and financial accounts, reviewing communications for fraudulent links and spoofed domains, investigating attempted Coinbase takeover activity, and spending substantial time attempting to verify official distribution instructions. Plaintiff will further itemize out-of-pocket costs and time through discovery and damages proof.

62. John Doe 1 has not received subsequent distributions after the Breach. His distribution delay is not a mere inconvenience. With a six-figure claim, the delay caused loss of use, lost time value, lost ability to control assets, increased security risk, and lost opportunity to deploy or safeguard funds during a volatile cryptocurrency market.

63. John Doe 1 has suffered anxiety, distress, nuisance, and loss of privacy because his name and contact information have been tied to a large cryptocurrency claim and used to target him through multiple channels. Those injuries are concrete and particularized, and they continue so long as Stretto fails to remediate the distribution and communications failures caused by the Breach.

CLASS ACTION ALLEGATIONS

64. Plaintiff brings this action under Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) on behalf of the following classes and subclasses, subject to refinement after discovery:

Nationwide April 2024 Stretto Security Incident Exposure Class:

All natural persons whose Bankruptcy Code PII or other personal, contact, claim, schedule, voting, account, or distribution information was accessed, exfiltrated, copied, or otherwise compromised in the April 2024 Stretto data-security incident involving bankruptcy matters administered by Stretto, including Celsius, Voyager, Prime Core, and any other affected bankruptcy case.

Targeted Attack Subclass:

All class members who, after the April 2024 incident, received Stretto-, estate-, debtor-, distribution-agent-, wallet-, or exchange-themed phishing, social-engineering, account-takeover, SIM-swap, wallet-drainer, postal-mail, text-message, telephone, or similar targeted attacks, or who suffered concrete mitigation costs, account takeover attempts, monetary losses, or other harms induced by such attacks.

Bankruptcy Process Loss Subclass:

All class members who suffered delayed, withheld, invalidated, reissued, failed, or otherwise impaired distributions, claim-code problems, account verification problems, support failures, lost time value, expungements, forfeitures, or other rights-critical process harms after Stretto's breach contaminated email and portal workflows.

65. Excluded from the classes are Defendant, its affiliates, parents, subsidiaries, officers, directors, employees, agents, and legal representatives; legal counsel for the parties; any judge presiding over this matter and the judge's immediate family and staff.

66. Numerosity is satisfied because the April 2024 Breach affected tens or hundreds of thousands of creditors. Stretto acknowledged approximately 104,000 affected Celsius creditors, and the Prime Core notice identified approximately 142,200 affected creditors. The full number of affected creditors across all impacted bankruptcy cases is known to Stretto and can be ascertained from Stretto's systems, notice logs, claims registers, affected-account lists, and investigation materials.

67. Commonality is satisfied because common questions of law and fact include: whether Stretto's employee-account security was reasonable; whether Stretto adequately secured CORE and related repositories; whether Stretto minimized, encrypted, segmented, and restricted creditor PII; whether Stretto timely identified and scoped affected data; whether Stretto timely notified affected creditors, estates, courts, and the United States Trustee; whether Stretto's post-Data Breach reliance on email and portal workflows was reasonable; whether Stretto should have deployed postal backstops, authenticity cues, phishing exemplars, takedowns, and support SLAs; whether Stretto's conduct caused targeted attacks and distribution delays; and what remedies are appropriate.

68. Predominance is satisfied because Stretto's security architecture, breach response, notification timing, communications design, distribution-support workflow, and remediation decisions were centralized and uniform. Those common issues will predominate over any individual issues. Individual damages can be determined through claims files, distribution logs, support tickets, account-status records, phishing reports, and ordinary damages proceedings.

69. Superiority is satisfied because maintaining this litigation as a class action will more efficiently and effectively allow Plaintiff and the Class to vindicate their rights and to obtain redress.

70. Typicality is satisfied because Plaintiff's claims arise from the same April 2024 Stretto Breach and the same post-Data Breach administration failures affecting the Class. Like the Class, Plaintiff had PII compromised, received targeted social-engineering attempts, incurred mitigation costs, and suffered distribution delay.

71. Adequacy is satisfied because Plaintiff's interests align with the class. Plaintiff seeks to hold Stretto responsible for costs caused by its own security and administration failures, not to reduce estate distributions or obtain relief at other creditors' expense. Plaintiff will fairly and adequately protect the interests of the classes and has retained counsel competent to prosecute complex data-breach, consumer, class-action, and bankruptcy-administration claims.

72. Rule 23(b)(2) certification is appropriate because Stretto acted or refused to act on grounds generally applicable to the class, making declaratory and injunctive relief appropriate.

73. Rule 23(b)(3) certification is appropriate because common questions predominate over individualized questions and a class action is superior to thousands of individual actions involving the same Breach, the same claims agent, and the same post-breach communication failures.

CLAIMS FOR RELIEF

COUNT I - NEGLIGENCE

(On behalf of Plaintiff and the Nationwide Class, or alternatively the Celsius, Targeted Attack, and Bankruptcy Process Loss Subclasses)

74. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

75. Stretto owed Plaintiff and the class duties independent of contract to exercise reasonable care in collecting, storing, using, securing, maintaining, and disposing of PII and claim data; to implement reasonable administrative, technical, and physical safeguards; to detect, contain, and remediate unauthorized access; to timely notify affected persons and courts; and to design post-breach communications reasonably calculated to reach creditors under the circumstances.

76. These duties arose from Stretto's role as a claims and noticing agent, from the Bankruptcy Code and Bankruptcy Court confidentiality regime, from Stretto's undertaking to administer claims and distributions for the benefit of creditors, from industry standards, and from Stretto's exclusive control over its security architecture and creditor-facing systems.

77. Stretto knew it possessed court-protected Bankruptcy Code PII for cryptocurrency creditors. Stretto knew that disclosure of names, emails, phone numbers, addresses, and claim information could enable phishing, social engineering, account takeover, and distribution theft. Stretto also knew that Celsius and Voyager creditors were actively receiving distribution communications and were susceptible to estate-branded impersonation. Stretto therefore had a duty to take reasonable measures to prevent the Data Breach and to secure Plaintiff's and the Class's data.

78. Stretto nevertheless breached those duties by, among other things, failing to employ security controls commensurate with the risk; failing to secure CORE and employee-account access; failing to segment and protect PII to prevent employee-account compromise; failing to to prevent exfiltration of creditor PII from its claims-administration systems; failing to follow reasonable incident-response procedures; delaying creditor notice; failing to promptly notify all affected courts; minimizing the exposure of names, addresses, emails, and phone numbers; failing to provide postal backstops and reliable authentication methods; failing to maintain support channels that provided individualized assistance; and failing to promptly cure distribution delays and account-status problems created or amplified by the breach.

79. After discovering suspicious activity on April 17, 2024, Stretto delayed creditor notice until May 7, 2024 or later, even though the compromised data could immediately be used for creditor impersonation attacks. Stretto also failed to promptly notify all affected courts and presiding judges until ordered by Judge Glenn.

80. Stretto continued to rely on a contaminated email channel and fragile support workflows during a period of active Stretto/estate impersonation. Stretto failed to promptly provide adequate postal backstops, phishing exemplars, clear authenticity cues, reliable telephone support, individualized distribution-status explanations, and rapid remediation of delayed distributions.

81. Indeed, Stretto's conduct was an extreme departure from ordinary care. Among other things, Stretto failed to adequately secure employee accounts and CORE access; failed to minimize, encrypt, segment, and restrict PII; failed to promptly notify affected creditors, courts, and the United States Trustee; failed to treat names, addresses, emails, and phone numbers as protected Bankruptcy Code PII; failed to provide reliable postal backstops and support after email

addresses were compromised; and failed to remediate distribution delays in a manner protecting high-value creditors like Plaintiff.

82. Stretto's gross negligence was especially egregious because the Bankruptcy Court had sealed precisely the information Stretto exposed, and because Judge Glenn had already recognized that disclosure of addresses, email addresses, and phone numbers posed serious risks to Celsius creditors.

83. Stretto's negligence foreseeably enabled third-party criminal conduct. Stretto knew that exposed crypto creditor PII would be used for phishing, social engineering, and account takeover. The intervention of criminal actors therefore does not break causation; it is the very risk that made Stretto's conduct negligent.

84. But for Stretto's breaches of duty, Plaintiff's PII would not have been exposed, Plaintiff would not have been targeted through estate- and exchange-themed social engineering, Plaintiff would not have incurred mitigation costs, and Plaintiff would not have suffered distribution delays and time-value losses.

85. As a direct and proximate result of Stretto's gross negligence, Plaintiff and the class suffered concrete injuries including exposure and loss of control of PII, targeted phishing and social-engineering attacks, account-takeover attempts, out-of-pocket mitigation costs, time costs, distribution delays, time-value losses, and emotional distress.

86. Stretto's conduct was willful, reckless, grossly negligent in disregard of a known, substantial risk to crypto creditors, including Plaintiff. Stretto's conduct directly and proximately caused exposure of PII, actual targeted attacks, mitigation costs, distribution delays, time-value losses, and emotional distress.

87. Plaintiff and the class are therefore entitled to compensatory, consequential, nominal, punitive, and other damages as permitted by law, together with injunctive relief and costs.

COUNT II – NEGLIGENT UNDERTAKING
(On behalf of Plaintiff and the Nationwide Class, or alternatively the Celsius, Targeted Attack, and Bankruptcy Process Loss Subclasses)

88. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

89. Stretto undertook to render services necessary for the protection of creditors and their property, including maintaining claims registers, preserving creditor PII, issuing notices, administering distribution communications, providing support, and processing or facilitating distributions.

90. Plaintiff and the class reasonably relied on Stretto's undertaking because Stretto was the official claims and noticing agent and controlled official creditor-facing systems. Creditors could not secure Stretto's systems, inspect Stretto's breach response, or independently design safer notice channels.

91. Stretto's negligent performance increased the risk of harm to Plaintiff and the class. It exposed PII, contaminated distribution communications, delayed notice, failed to provide alternate reliable channels, and made it harder for creditors to distinguish legitimate instructions from fraudulent lures.

92. Stretto's negligent undertaking directly and proximately caused Plaintiff and the class injuries, including actual targeted misuse of PII, attempted Coinbase account takeover, mitigation costs, delayed distributions, and time-value losses.

93. Stretto's conduct was willful, reckless, grossly negligent in disregard of a known, substantial risk to crypto creditors, including Plaintiff. Stretto's conduct directly and proximately

caused exposure of PII, actual targeted attacks, mitigation costs, distribution delays, time-value losses, and emotional distress.

COUNT III – BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Nationwide Class, or alternatively the Celsius, Targeted Attack, and Bankruptcy Process Loss Subclasses)

94. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

95. As a court-approved claims and noticing agent and estate professional performing functions in place of the Clerk's Office, Stretto owed fiduciary or fiduciary-like duties of loyalty, care, candor, and faithful administration to the estates for the benefit of creditors, and to known creditors in matters within the scope of Stretto's official undertaking.

96. Those duties included safeguarding creditor PII, complying with confidentiality and sealing orders, promptly informing the Court and affected creditors of material compromises, designing notice reasonably calculated to reach known creditors, avoiding self-protective minimization of breaches, and administering distribution-related communications without exposing creditors to avoidable harm.

97. Stretto breached those duties by failing to protect PII, failing to promptly notify affected creditors and courts, minimizing the significance of exposed Bankruptcy Code PII, failing to implement safe post-breach communications and support, and failing to remediate distribution process harms caused by the breach.

98. Stretto's breaches caused non-derivative injuries to Plaintiff and the class, including targeted attacks, attempted account takeover, mitigation costs, loss of control over PII, distribution delays, and time-value losses. Plaintiff seeks damages and equitable relief from Stretto, not from any bankruptcy estate.

99. Stretto's conduct was willful, reckless, grossly negligent in disregard of a known, substantial risk to crypto creditors, including Plaintiff. Stretto's conduct directly and proximately caused exposure of PII, actual targeted attacks, mitigation costs, distribution delays, time-value losses, and emotional distress.

COUNT IV - BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class, or alternatively the Celsius, Targeted Attack, and Bankruptcy Process Loss Subclasses)

100. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

101. By accepting Plaintiff's and the class's PII and claim information for claims administration, notices, creditor support, and distributions, and by presenting itself as the official claims and noticing agent through which creditors had to receive and act on distribution-critical information, Stretto entered into implied-in-fact obligations with creditors.

102. Those implied obligations included maintaining reasonable security for creditor PII, using the PII only for authorized claims and distribution purposes, providing communications reasonably calculated to reach creditors, and administering post-breach support and distribution workflows in a manner that did not render creditors unable to safely claim distributions.

103. Plaintiff and the class provided valuable PII, time, claims information, account information, and cooperation. Stretto accepted those benefits, used them to perform paid bankruptcy-administration work, and charged the estates for services premised on safe custody and use of creditor data.

104. Stretto breached its implied contractual obligations by exposing PII, failing to provide reasonable security, failing to timely notify, failing to implement reliable post-breach

channels, and failing to provide adequate support to resolve distribution issues after the email channel was contaminated.

105. As a direct and proximate result, Plaintiff and the class did not receive the benefit of Stretto's promised safe claims-administration services and suffered damages including mitigation costs, delayed distributions, time-value losses, and other consequential damages.

COUNT V - BREACH OF CONFIDENCE
(On behalf of Plaintiff and the Nationwide Class, or alternatively the Celsius, Targeted Attack, and Bankruptcy Process Loss Subclasses)

106. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

107. Plaintiff and the class had a privacy and property interest in their PII and claim information. That information was conveyed to or held by Stretto in confidence for limited claims-administration and distribution purposes.

108. Stretto knew the information was confidential. The Bankruptcy Court sealed addresses, email addresses, phone numbers, and related information because disclosure would expose creditors to phishing, threats, and unlawful injury. Stretto's position as claims agent depended on the trust that it would maintain confidentiality.

109. Stretto breached the confidence owed to Plaintiff and the class by failing to safeguard the information and by allowing unauthorized access, exfiltration, and misuse.

110. As a direct and proximate result, Plaintiff and the class suffered loss of privacy, loss of control of PII, targeted attacks, mitigation costs, distribution delays, time-value losses, anxiety, distress, and other damages.

COUNT VI - DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiff and the Nationwide Class, or alternatively the Celsius, Targeted Attack, and Bankruptcy Process Loss Subclasses)

111. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

112. An actual controversy exists regarding Stretto's present and continuing duties to protect creditor PII, remediate the April 2024 breach, administer safe post-breach communications, and prevent ongoing distribution process harms.

113. Plaintiff seeks narrow, time-limited relief directed to Stretto and funded by Stretto so that creditor distributions are not reduced. The requested relief is consistent with the objectives of the bankruptcy estates and does not alter any confirmed plan or distribution entitlement.

114. Plaintiff requests an injunction requiring Stretto to implement, at its expense, a remedial program that includes:

a. USPS First-Class Mail backstops for all rights-critical and distribution-critical notices to affected creditors, including creditors with bounced emails, open claim codes, distribution failures, Coinbase/PayPal/KYC issues, high-value claims, support tickets older than seven days, or unresolved post-breach status changes;

b. publication of side-by-side "legitimate versus spoof" exemplars on case websites and dockets, including examples of fake wallet-connection emails, fake distribution sites, fake support calls, and postal-mail scams;

c. clear domain and sender-authenticity cues, including SPF, DKIM, and DMARC enforcement, with a published list of official domains and email addresses and a warning that creditors will never be asked to connect a wallet or provide credentials by email;

d. rapid lookalike-domain and fake-portal takedown procedures, with documented service-level agreements and quarterly reporting to the Court;

e. a dedicated live support channel and escalation process for affected high-value creditors and creditors reporting account-takeover attempts, with individualized responses rather than boilerplate ticket closures;

f. audit logs and explanations for distribution status changes, invalidated claim codes, reissued codes, failed distribution attempts, and support-ticket outcomes;

g. a process to review and remediate creditors, including Plaintiff, who received an initial distribution before the breach but did not receive subsequent distributions after the Breach;

h. phishing-resistant multi-factor authentication, least-privilege access, encryption at rest, data minimization, data-loss prevention, and independent security assessment for systems holding bankruptcy PII;

i. a prominent statement on Stretto case websites that use of Stretto websites or portals to obtain case information does not waive Data Breach claims or impose arbitration for claims arising from the April 2024 Breach; and

j. quarterly reports summarizing backstop mailings, undeliverable emails, unresolved support tickets, spoof takedowns, security remediation, and distribution remediation efforts.

115. Plaintiff also seeks a declaration that Stretto owed duties to protect Bankruptcy Code PII and to administer post-breach notices and distributions in a manner reasonably calculated to reach known creditors under the circumstances, and that Stretto breached those duties.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed classes and subclasses, respectfully requests that the Court:

(a) Certify the proposed classes and subclasses under Rule 23 and appoint Plaintiff as class representative and his counsel as class counsel;

(b) Grant judgment in favor of Plaintiff and the classes on all claims;

(c) Award compensatory, consequential, nominal, punitive where available, restitution, and other damages in amounts to be proven at trial;

(d) Award pre-judgment and post-judgment interest;

(e) Enter declaratory and injunctive relief requiring Stretto to remediate the breach and post-breach distribution harms at Stretto's expense;

(f) Award reasonable attorneys' fees, expert fees, and costs to the extent permitted by law;

(g) Order any other equitable relief necessary to ensure that remediation costs do not reduce creditor distributions; and

(h) Grant such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: April 27, 2026

Respectfully submitted,

HAUSFELD LLP

By: */s/Renner K. Walker*

Renner K. Walker
rwalker@hausfeld.com
Steven M. Nathan
snathan@hausfeld.com
33 Whitehall St., 14th Floor
New York, NY 10004
Tel: 646-357-1100
Fax: 212-202-4322

James J. Pizzirusso*
jpizzirusso@hausfeld.com
HAUSFELD LLP
1200 17th Street N.W.
Suite 600
Washington, DC 20036
Tel: 202-540-7200
Fax: 202-540-7201

Nicholas Andrew Hall*
nhall@hallattorneys.com
HALL ATTORNEYS, P.C.
P.O. Box 1370
Edna, Texas 77957
+1 713 428 8967

Counsel for Plaintiff and the Putative Class

*Pro Hac Vice application forthcoming