

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street, 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for the New Jersey Division of Consumer Affairs

FILED

November 10 2021

Division of Consumer Affairs

By: Thomas Huynh
Deputy Attorney General
(862) 350-0165

Gina Pittore
Deputy Attorney General
(845) 323-8333

STATE OF NEW JERSEY
DEPARTMENT OF LAW AND PUBLIC
SAFETY DIVISION OF CONSUMER AFFAIRS

In the Matter of

COMMAND MARKETING
INNOVATIONS, LLC AND
STRATEGIC CONTENT IMAGING,
LLC,

Respondents.

Administrative Action

CONSENT ORDER

WHEREAS this matter having been opened by the New Jersey Division of Consumer Affairs, Office of Consumer Protection (“Division”), as an investigation to ascertain whether violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 to -226 (“CFA”), and/or the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, and the Department of Health and Human Services Regulations, 45 C.F.R. § 160 to 180 (collectively, “HIPAA”) have been or are being committed (the “Investigation”) by Command Marketing Innovations, LLC and Strategic Content Imaging, LLC (collectively, “Respondents”);

WHEREAS the Attorney General is charged with the responsibility of enforcing the CFA, and the Director of the Division is charged with administering the CFA on behalf of the Attorney General;

WHEREAS the Attorney General, as *parens patriae* for the State of New Jersey and in its sovereign capacity, may, pursuant to 42 U.S.C. § 1320d-5(d), enforce the provisions of HIPAA;

WHEREAS Command Marketing Innovations, LLC (“CMI”) is a Garfield, New Jersey-based company that provides print and marketing solutions to its clients;

WHEREAS Strategic Content Imaging, LLC (“SCI”) is a Secaucus, New Jersey-based company that provides digital print, finishing, and fulfillment services to businesses;

WHEREAS the Division alleges that Respondents violated the CFA and HIPAA in connection with the improper disclosure and failure to protect the confidentiality of Personal Information, Protected Healthcare Information, and/or Electronic Protected Healthcare Information from October 31, 2016, through November 2, 2016, which impacted approximately 55,715 New Jersey residents;

WHEREAS the Division and Respondents (collectively, the “Parties”) have reached an amicable agreement resolving the issues in controversy and concluding the Investigation without the need for further action, and Respondents having cooperated with the Investigation and consented to the entry of this order (“Consent Order”) without admitting any violation of law, and for good cause shown;

IT IS ORDERED AND AGREED as follows:

1. EFFECTIVE DATE

1.1 This Consent Order is effective on the date that it is filed with the Division, which filing date the Division Clerk stamps on the executed Consent Order (“Effective Date”).

2. DEFINITIONS

As used in this Consent Order, the following words or terms shall have the following meanings, which shall apply wherever the words or terms appear in this Consent Order:

2.1 “Attorney General” shall refer to the Attorney General of the State of New Jersey and the Office of the Attorney General of the State of New Jersey.

2.2 “Breach” shall refer to the Security Incident, and all events related thereto, discovered by Respondents on or about November 2, 2016, and publicly announced on November 14, 2016, which exposed the PI, PHI and/or ePHI of approximately 55,715 New Jersey residents.

2.3 “Breach Notification Rule” shall be defined in accordance with 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and D.

2.4 “Business Associate” shall be defined in accordance with 45 C.F.R. § 160.103.

2.5 “Business Associate Agreement” or “BAA” shall mean the contract or other written arrangement required by 45 C.F.R. § 164.502(e)(2) and that meets the requirements of 45 C.F.R. §164.504(e).

2.6 “CMI” shall mean Command Marketing Innovations, LLC, its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers, and employees doing business in the United States.

2.7 “Covered Entity” shall be defined in accordance with 45 C.F.R. § 160.103.

2.8 “Customer” shall refer to a leading New Jersey-based managed healthcare organization with whom CMI executed a BAA and for whom CMI agreed to provide mailing, fulfillment, and printing services, including the printing and mailing of EOB statements.

2.9 “Division” or “Division of Consumer Affairs” shall refer to the New Jersey Division of Consumer Affairs.

2.10 “Electronic Protected Health Information” or “ePHI” shall be defined in accordance with 45 C.F.R. § 160.103.

2.11 “Explanation of Benefit Statements” or “EOBs” are paper or electronic documents that healthcare plan members receive after a healthcare claim is processed. The EOB may include members’ names, member identification numbers, claim numbers, dates of service, limited description of services, service codes, and/or provider/facility names.

2.12 “New Jersey” or “State” shall refer to the State of New Jersey.

2.13 “Personal Information” or “PI” shall mean the data elements in the definition of personal information set forth in the Identity Theft Protection Act, N.J.S.A. 56:8-161 to 166.3.

2.14 “Privacy Rule” shall refer to 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

2.15 “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 106.103.

2.16 “SCI” shall mean Strategic Content Imaging, LLC, its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers, and employees doing business in the United States.

2.17 “Security Incident” shall be defined in accordance with 45 C.F.R. § 106.103.

2.18 “Security Rule” shall be defined in accordance with 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

3. STIPULATED FACTS

3.1 CMI was incorporated in New Jersey in 2016, and maintains a principal business address at 70 Outwater Lane, Garfield, New Jersey 07026.

3.2 SCI was incorporated in New Jersey in 2001, and maintains a principal business address at 100 Castle Road, Secaucus, New Jersey 07094.

3.3 At all relevant times, CMI is and has been a Covered Entity and Business Associate within the meaning of HIPAA, and SCI is and has been a Business Associate within the meaning of HIPAA.

3.4 As a Covered Entity and Business Associate, CMI is required to comply with the HIPAA federal standards that govern the privacy of PHI, including the Privacy Rule and the Security Rule.

3.5 As a Business Associate, SCI is required to comply with the HIPAA federal standards that govern the privacy of PHI, including the Privacy Rule and the Security Rule.

3.6 On or about September 1, 2016, the Customer and CMI executed a Business Associates Agreement (“BAA”) for CMI to provide mailing, fulfillment, and printing services to the Customer, including the printing and mailing of EOB statements for the Customer’s members.

3.7. In the BAA, the parties established CMI’s obligations as a Business Associate, including CMI’s duty to comply with the HIPAA Security Rule and “implement and use all appropriate safeguards to protect the privacy of [PHI.]”

3.8. The BAA also required CMI to: (a) enter into written agreements with all agents and subcontractors to whom CMI provides PHI, requiring the agents or subcontractors to agree to the same restrictions and conditions with respect to PHI; (b) carry out adequate due diligence on each agent or subcontractor to ensure that it is capable of providing the level of protection required for the PHI and provide evidence of such due diligence to the Customer upon request;

and (c) remain liable for all acts and/or omissions of the agent or subcontractor.

3.9 On or about September 9, 2016, CMI executed a BAA with SCI, for SCI to assist CMI in providing fulfillment and printing services to the Customer, specifically the printing of EOBS.

3.10. In the BAA, CMI acknowledged it was subject to obligations as a HIPAA covered entity, including its duty to “[n]ot use or disclose [PHI] in any manner that would not be permissible under [HIPAA]” and “comply with all HIPAA Rules[.]”

3.11. As a Business Associate of CMI, SCI agreed in relevant part to: (a) not use or disclose PHI other than as permitted; (b) use appropriate safeguards and comply with 45 C.F.R. §§ 164.302 through 164.318, to prevent the unauthorized use or disclosure of PHI; and (c) report to CMI any unauthorized use or disclosure of PHI, including breaches of unsecured PHI and Security Incidents.

3.12. In late October and early November 2016, without notifying the Customer or CMI, SCI changed its printing process by increasing the size of the paper it used to print. SCI did not conduct sufficient quality control checks before SCI amended its printing process. The change caused the front page of one member’s EOB to become associated with the back page of another member’s EOB. SCI’s quality assurance system failed to identify this mistake because the system only checked front pages, not back pages, for errors. CMI did not detect this error prior to mailing.

3.13 On or about November 2, 2016, the Customer notified SCI of a potential printing error that disclosed the PHI of Horizon’s members. Specifically, the Customer’s members received EOBS that contained the PHI of other members.

3.14. That same day, SCI halted production on all EOBS and similar print campaigns and investigated the issue.

3.15 The printing error affected EOB statements mailed from October 31 through November 2, 2016, and impacted approximately 55,715 of the Customer's members located in New Jersey.

3.16 The printing error disclosed member identification numbers, claims numbers, dates of service, descriptions of services provided, and service codes and/or provider/facility names.

3.17 On or about November 14, 2016, CMI notified the New Jersey State Police and the affected population of the Breach.

3.18 Respondents stipulate to the enumerated facts stated in Section 3 for purposes of this Consent Order only.

4. ALLEGED VIOLATIONS OF LAW

4.1 The Division has alleged the following:

- a. At all relevant times set forth in Section 3 above (the "Relevant Time Period"), incorporated herein by reference, CMI was and continues to be a Covered Entity.
- b. During the Relevant Time Period, CMI was and continues to be a Business Associate of the Customer.
- c. During the Relevant Time Period, SCI was and continues to be a Business Associate of CMI.
- d. As a Covered Entity and Business Associate, CMI was, and continues to be, required to comply with HIPAA standards governing the privacy and security of PHI and/or ePHI, including, but not limited to the Security Rule and the Privacy Rule.

- e. As a Business Associate, SCI was, and continues to be, required to comply with HIPAA standards governing the privacy and security of PHI and/or ePHI, including, but not limited to the Security Rule and the Privacy Rule.
 - f. Respondents violated the CFA, HIPAA's Security Rule, and HIPAA's Privacy Rule when they failed to protect the confidentiality of PHI and ePHI, resulting in the Breach that exposed the PI, PHI, and ePHI of 55,715 of the Customer's members located in New Jersey.
 - g. Specifically, Respondents failed to comply with the Security Rule and Privacy Rule by:
 - failing to ensure the confidentiality of ePHI, in violation of 45 C.F.R. § 164.306(a)(1);
 - failing to protect against a reasonably anticipated, unauthorized disclosure of PHI contained in EOBs, in violation of 45 C.F.R. 164.306(a)(3); and
 - failing to review and modify security measures as needed to continue reasonable and appropriate protection of ePHI, in violation of 45 C.F.R. § 164.306(e).
 - h. At all relevant times, Respondents Advertised, offered for Sale, or Sold Merchandise, including services, within the meaning of the CFA.
 - i. Respondents' failure to protect the confidentiality of 55,715 New Jersey residents' PHI and ePHI constitute separate and additional unconscionable commercial practices in violation of the CFA, N.J.S.A. 56:8-2.
- 4.2 Respondents deny the Division's alleged violations of law in Section 4.1.

5. AGREED-UPON BUSINESS PRACTICES

A. Compliance with State and Federal Law

5.1 Respondents shall not engage in conduct in violation of the CFA and HIPAA, including the Privacy Rule, Breach Notification Rule and/or Security Rule, in connection with the security, collection, use, disclosure, or storage of PI, PHI, or ePHI.

5.2 SCI shall become certified by the Health Information Trust Alliance (“HITRUST”) within one hundred and twenty (120) days of the Effective Date, if not already certified as of the Effective Date, and shall annually maintain HITRUST certification.

5.3 CMI certifies that as a part of its current business operations, CMI does not create, receive, maintain, or transmit PHI or ePHI. To the extent CMI’s business operations change in any way which causes CMI to create, receive, maintain, or transmit PHI or ePHI, CMI shall become certified by HITRUST before creating, receiving, maintaining, or transmitting ePHI.

5.4 Respondents shall each implement and maintain a Security Information and Event Management (“SIEM”) tool to identify and track all aspects of their IT infrastructure to identify vulnerabilities and threats.

5.5 Respondents shall each maintain and regularly update policies related to Corrective and Preventative Actions, Risk Management, Change Management, Onboarding, and Training.

5.6 Respondents shall each appoint one (1) employee as its Chief Information Security Officer (“CISO”), within one hundred and twenty (120) days of the Effective Date, if not already appointed as of the Effective Date. The CISO shall have the background and expertise, with documentation of her or his background and expertise, in information security appropriate to the level, size, and complexity of her or his role in implementing, maintaining, and monitoring the information security program. The CISO shall also, on an annual basis, obtain information security training and maintain documentation of all training received.

5.7 Respondents shall each appoint one (1) employee as its Chief Privacy Officer, within one hundred and twenty (120) days of the Effective Date, if not already appointed as of the Effective Date. The Chief Privacy Officer shall have the background and expertise, with documentation of her or his background and expertise, in HIPAA compliance appropriate to the level, size, and complexity of her or his role in implementing, maintaining, and monitoring HIPAA compliance. The Chief Privacy Officer shall also, on an annual basis, obtain HIPAA compliance training and maintain documentation of all training received.

5.8 Respondents shall each appoint one (1) employee as its Director of Compliance and Quality Assurance within one hundred and twenty (120) days of the Effective Date, if not already appointed as of the Effective Date.

5.9 Respondents shall subscribe to a personalized security awareness and anti-phishing training program within one hundred and twenty (120) days of the Effective Date, if not already done as of the Effective Date, and use these programs to train their employees.

5.10 Respondents shall obtain formal approval from a Covered Entity before executing any material changes to their printing process, including but not limited to the printing of EOBs.

5.11 Respondents shall establish a Change Advisory Board (“CAB”), comprising all members of SCI’s Executive Team, including representatives from Operations, Human Resources, Administration, Client Services, Information Technology, and related Subject Matter Experts, that shall meet to discuss all changes to SCI’s printing process, within one hundred and twenty (120) days of the Effective Date, if not already established as of the Effective Date.

5.12 SCI shall implement an issue tracking system to keep detailed records of Information Technology and Development-related tasks within one hundred and twenty (120) days of the Effective Date, if not already implemented as of the Effective Date.

6. SETTLEMENT PAYMENT

6.1 The Parties have agreed to a monetary settlement to resolve the Investigation in the amount of \$130,000.00 (“Settlement Payment”), with \$65,000.00 suspended so long as Respondents abide by the terms of this Consent Order. The Settlement Payment shall be allocated seventy-five (75) percent to SCI and twenty-five (25) percent to CMI. The entirety of the Settlement Payment is allocated to the Division’s civil penalty claims. The allocation of the Settlement Payment is not a finding by the Division or an admission by Respondents of liability for civil penalties.

6.2 Respondents shall remit the unsuspended portion of the Settlement Payment within fifteen (15) days after the Effective Date.

6.3 Respondents shall make the Settlement Payment by wire transfer, credit card, or by certified check, cashier’s check or money order made payable to the “New Jersey Division of Consumer Affairs” and forwarded to:

Case Initiation and Tracking Unit
New Jersey Department of Law and Public Safety
Division of Consumer Affairs
124 Halsey Street – 7th Floor
P.O. Box 45025
Newark, New Jersey 07101
Attention: Aziza Salikhova, Lead Investigator

6.4 Upon making the Settlement Payment, Respondents shall immediately be fully divested of any interest in, or ownership of, the money paid. All interest in the Settlement Payment, and any subsequent interest or income derived therefrom, shall inure entirely to the benefit of the Division pursuant to the terms herein.

7. GENERAL PROVISIONS

7.1 This Consent Order is entered into by the Parties as their own free and voluntary act and with full knowledge and understanding of the obligations and duties imposed by this Consent Order.

7.2 This Consent Order shall be governed by, and construed and enforced in accordance with, the laws of the State of New Jersey.

7.3 The Parties have negotiated, jointly drafted, and fully reviewed the terms of this Consent Order and the rule that uncertainty or ambiguity is to be construed against the drafter shall not apply to the construction or interpretation of this Consent Order.

7.4 This Consent Order contains the entire agreement among the Parties. Except as otherwise provided herein, this Consent Order shall be modified only by a written instrument signed by or on behalf of the Parties.

7.5 Except as otherwise explicitly provided in this Consent Order, nothing herein shall be construed to limit the authority of the Attorney General to protect the interests of the State or the people of the State.

7.6 If any portion of this Consent Order is held invalid or unenforceable by operation of law, the remaining terms of this Consent Order shall not be affected.

7.7 This Consent Order shall be binding upon the Parties and their successors in interest. In no event shall assignment of any right, power, or authority under this Consent Order avoid compliance with this Consent Order.

7.8 This Consent Order is entered into by the Parties for settlement purposes only. Neither the fact of nor any provision contained in this Consent Order shall constitute or be construed as: (a) an approval, sanction, or authorization by the Attorney General, the Division, or any other governmental unit of the State of any act or practice of Respondents; or (b) an

admission by Respondents that they violated the CFA or HIPAA, including the Privacy Rule, Breach Notification Rule, and/or the Security Rule, or any other federal or State law, administrative rule or regulation, or an express or implied admission of any other matter of fact or law, or of any liability or wrongdoing.

7.9 This Consent Order is not intended, and shall not be deemed, to constitute evidence or precedent of any kind in any action or proceeding except in: (a) an action or proceeding by one of the Parties to enforce, rescind, or otherwise implement any or all of the terms herein; or (b) an action or proceeding involving a Released Claim (as defined in Section 8) to support a defense of res judicata, collateral estoppel, release, or other theory of claim preclusion, issue preclusion, or similar defense.

7.10 The Parties represent and warrant that their signatories to this Consent Order have authority to act for and bind the respective Party.

7.11 Unless otherwise prohibited by law, any signatures by the Parties required for filing of this Consent Order may be executed in counterparts, each of which shall be deemed an original, but all of which shall constitute one and the same Consent Order. Electronic signatures shall constitute acceptable, binding signatures for purposes of this Consent Order.

8. RELEASE

8.1 In consideration of the undertakings, mutual promises, and obligations provided for in this Consent Order and conditioned on Respondents making the Settlement Payment as described in Section 6, the Division hereby agrees to release Respondents from any and all civil claims or causes of action, or consumer-related administrative claims or actions, to the extent permitted by law, which the Division could have brought prior to the Effective Date against Respondents for violations of any consumer protection law administered or enforced by the Division, CFA or HIPAA, including the Privacy Rule, Breach Notification Rule, and/or Security

Rule, arising out of the Investigation, as well as the matters specifically addressed in this Consent Order (“Released Claims”).

8.2 Notwithstanding any term of this Consent Order, the following do not comprise Released Claims: (a) private rights of action; (b) actions to enforce this Consent Order; and (c) any claims against Respondents by any other agency or subdivision of the State except any civil claims or causes of action, or consumer-related administrative claims or actions, arising out of the Investigation as well as the matters specifically addressed in this Consent Order that the Division could have brought but has released in Section 8.1 above.

9. PENALTIES FOR FAILURE TO COMPLY

9.1 The Attorney General (or designated representative) shall have the authority to enforce the provisions of this Consent Order or to seek sanctions for violations hereof or both.

9.2 Prior to filing any action to enforce the provisions of this Consent Order, the Attorney General (or designated representative) shall meet and confer with Respondents in an attempt to resolve any dispute with respect to compliance with this Consent Order. The Attorney General (or designated representative) shall notify Respondents in writing of the alleged violation of this Consent Order, and Respondents shall have fifteen (15) days to respond to the notification. The Attorney General (or designated representative) shall not file any action until the fifteen (15) days expire.

10. COMPLIANCE WITH ALL LAWS

10.1 Except as provided in this Consent Order, no provision herein shall be construed as:

- a. Relieving Respondents of their obligations to comply with all State and federal laws, regulations, or rules, as now constituted or as may hereafter be amended; granting permission to engage in any acts or practices prohibited by any such laws, regulations, or rules; or requiring Respondents to take an action that is prohibited

by such laws, regulations, or rules; or

- b. Limiting or expanding any right the Division may otherwise have to obtain information, documents, or testimony from Respondents pursuant to any State or federal law, regulation, or rule, as now constituted or as may hereafter be amended, or limiting or expanding any right Respondents may otherwise have pursuant to any State or federal law, regulation, or rule, to oppose any process employed by the Division to obtain such information, documents, or testimony.

11. NOTICES

11.1 Except as otherwise provided herein, any notices or other documents required to be sent to the Division or Respondents pursuant to this Consent Order shall be sent by electronic mail and United States mail, Certified Mail Return Receipt Requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the documents. The notices and/or documents shall be sent to the following addresses:

For the Division:

Thomas Huynh and Gina Pittore
Deputy Attorneys General
Office of the Attorney General
Department of Law and Public Safety
124 Halsey Street, 5th Floor
Newark, New Jersey 07101
Thomas.Huynh@law.njoag.gov and Gina.Pittore@law.njoag.gov

For Respondents:

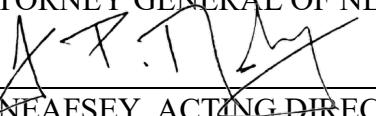
Claudia McCarron, Esq.
Richard Haggerty, Esq.
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, Pennsylvania 19333
CMccarron@mullen.law

With copies to
Loren Breslow, President
Command Marketing Innovations
883 Apache Road
Franklin Lakes, New Jersey 07417

Nicholas Brusco, President
Strategic Content Imaging
100 Castle Road
Secaucus, New Jersey 07094

IT IS ON THE 10th DAY OF November, 2021 SO ORDERED.

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY

By: 
SEAN P. NEAFSEY, ACTING DIRECTOR
DIVISION OF CONSUMER AFFAIRS

THE PARTIES CONSENT TO THE FORM, CONTENT AND ENTRY OF THIS CONSENT ORDER ON THE DATES ADJACENT TO THEIR RESPECTIVE SIGNATURES.

FOR THE DIVISION:

ANDREW J. BRUCK
ACTING ATTORNEY GENERAL OF NEW JERSEY

By: /s/ Thomas Huynh

Thomas Huynh
Deputy Attorney General
124 Halsey Street, 5th Floor
Newark, New Jersey 07101
Thomas.Huynh@law.njoag.gov

Dated: November 8, 2021

FOR RESPONDENTS CMI AND SCI:

By: Richard Haggerty

Richard Haggerty, Esq.
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, Pennsylvania 19333
rhaggerty@mullen.law

Dated: November 8, 2021