

**BEFORE THE COMMISSIONER OF SECURITIES AND INSURANCE,
OFFICE OF THE MONTANA STATE AUDITOR**

IN THE MATTER OF

JOHN OR JANE DOE USING THE
ALIAS BAILLIE (BAILEY) GIFFORD,

Respondent.

Case No. SEC-2026-00070

**FINAL AGENCY ACTION AND
DEFAULT ORDER**

On April 15, 2026, the Commissioner of Securities and Insurance, Office of the Montana State Auditor (“Commissioner”), served a Notice of Proposed Agency Action and Opportunity for Hearing (“NOPAA”) on Respondent, Baillie (Bailey) Gifford, collectively by email at the address provided.

CSI has not received a written hearing request from the Respondent. A copy of the NOPAA is attached as Exhibit A. The NOPAA provided the Respondent with an opportunity for an administrative hearing if requested within 24 days of service of the NOPAA. Therefore, the deadline for the Respondent to request an administrative hearing to challenge the NOPAA was May 9, 2026. The NOPAA also warned that failure to respond and request a hearing by the deadline would result in a default order.

More than 24 days have elapsed since the date of the NOPAA and no request for hearing has been received. Therefore, a default order will be issued under Admin. R. Mont. 1.3.214. The Commissioner considered the evidence and exhibits and makes the following determinations:

FINDINGS OF FACT

1. On January 9, 2025, CSI received a complaint from R.P., a Montana resident over the age of 60, who reported that he was the victim of securities fraud. This matter was investigated by CSI Investigator Ryan Sullivan

2. On or about June 2024, Respondent, identifying herself as "Baillie Gifford" (also known as "Bailey Gifford"), represented by email to R.P. that her purported firm, "Bailey Gifford Capital," had purchased accounts from Goldman Sachs. R.P. has since confirmed with the legitimate Baillie Gifford & Co. investment firm located in England that he was defrauded by an individual falsely claiming association with, or imitating, the legitimate firm.

3. In ongoing email communications, Respondent presented R.P. with a purported cryptocurrency investment opportunity. At Respondent's direction, R.P. transmitted funds through wire transfers, peer-to-peer payment applications including Cash App, and cryptocurrency exchanges such as Crypto.com, to accounts that were specifically identified by Respondent as the destinations for those deposits. R.P. understood these transactions to be part of an investment strategy to grow his retirement savings.

4. Through websites provided by Respondent-bailliemain.com and baillieglobalmarkets.com (both of which are no longer accessible)-R.P. was led to believe that his investments had grown to more than \$3,000,000. Respondent reinforced this belief by granting R.P. access to the websites that showed the account balance was increasing and maintaining regular electronic communication, thereby creating the false appearance that R.P.'s investments were generating substantial returns.

5. After making several investments without difficulty, R.P. attempted to withdraw funds but instead received messages on the platform indicating that his account had been frozen. The messages purported to be from "Online Services" and stated the withdrawal was being delayed because of alleged regulatory violations, including "money laundering." R.P. was instructed to make additional deposits of up to \$336,405.13, to bring his total balance to \$2,803,376.15. He was instructed to provide additional personal

identification, letters, and video verification as purported requirements to "verify" that his account was not at risk. R.P. had to borrow money from friends to provide the additional money that he believed was necessary to withdraw his investments.

6. Respondent directed R.P. to make investments into bank accounts at Banco Sabadell in Miami, Florida, and Flagstar Bank in Hicksville, New York, held by an individual, B.W.W., domiciled in Michigan. These transactions included three large wire transfers in the amounts of \$40,000, \$90,000, and \$149,000 plus fees to the Banco Sabadell account, and three additional wire transfers in the amounts of \$140,152, \$150,000, and \$165,670 to the Flagstar account.

7. Subpoenaed Flagstar Bank records show that three deposits into B.W.W.'s account were traceable to R.P., and that large, rapid in-and-out wire transfers reflected a pattern consistent with the use of a third-party "money mule." A third-party "money mule" is an individual whose financial accounts are used as an intermediary to receive, move, and transfer criminal proceeds, making the underlying fraudsters more difficult to detect and trace. This account was closed following a final withdrawal on February 21, 2025.

8. Another account held by B.W.W., jointly with an individual, C.W., showed small deposits and a transfer to the first account, followed by a final closeout.

9. The transactional patterns across these accounts indicate that B.W.W.'s accounts were used primarily as conduits to launder and obscure criminal proceeds associated with the underlying cryptocurrency fraud.

10. On February 20, 2026, Investigator Sullivan spoke with B.W.W., who stated that he had been recruited online into a purported investment and gold-trading opportunity by a woman who claimed her father owned a furniture store. He told Investigator Sullivan that he provided his banking information, invested his own funds, became a "VIP" and was promised approximately \$26 million in returns, ultimately losing approximately \$1.5 to \$1.6 million after liquidating his IRA and refinancing his home.

11. B.W.W. acknowledged that more than \$400,000 belonging to R.P. was routed through his accounts, with those funds ultimately transferred to Barclays Bank.

12. Respondent is not registered with the Commissioner as an investment advisor with CSI.

13. R.P. never regained access to his funds, and the circumstances indicate that he fell victim to a "pig butchering" fraud scheme. Respondent presented what appeared to be a legitimate investment opportunity, built trust over time, and provided detailed guidance on opening and funding the trading account. This type of scheme typically employs fake websites or account dashboards that falsely depict trading activity and profits, while the victim's funds are diverted to accounts controlled by the fraudster, leaving the victim unaware until attempting to withdraw funds.

14. Respondent provided or facilitated fraudulent investment advice for her own financial gain through a scheme that operated by directing transfers to accounts owned or controlled by Respondent.

CONCLUSIONS OF LAW

1. The Commissioner has jurisdiction over this matter and is tasked with enforcement of the Securities Act of Montana, pursuant to §§ 30-10-101 through 30-10-342, MCA.

2. The Commissioner is entrusted to protect investors, persons engaged in securities, and the public interest. § 30-10-102, MCA.

3. It is unlawful for any person, in connection with the offer, sale, or purchase of any security, whether directly or indirectly, to employ any device, scheme, or artifice to defraud, make any untrue statement of material fact, (or omit a material fact necessary to prevent any other statements from being misleading), or engage in any act, practice, or course of business that operates or would operate as a fraud or deceit on any person. § 30-10-301(2), MCA.

4. "[A]ny person that knowingly provides substantial assistance to another person in violation of a provision of [Title 30, Chapter 10, Part 23] must be considered to

be in violation of that provision to the same extent as the person to whom the assistance is provided.” § 30-10-321, MCA

5. R.P. is older than 60 years of age and is thus a "vulnerable person" pursuant to § 30-10-103(27)(a), MCA.

6. The Commissioner may impose a fine not to exceed \$20,000 per violation on a person found to have engaged in any act or practice constituting a violation of the Securities Act or a rule or order of the Commissioner and affecting a vulnerable person. § 30-10-305(3), MCA.

7. After conducting a hearing under § 33-1-701, MCA, the Commissioner may also impose an order of restitution on any person found to have violated § 30-10-301, MCA, with 10% annual interest from the date of violation, reasonable attorney fees, and costs associated with bringing the administrative action. § 30-10-309(1), MCA.

8. Respondent impersonated a legitimate investment firm, developing trust with R.P. and inducing him to invest money, provide sensitive personal and financial information in response to fabricated "regulatory reviews" and "compliance holds," and then misappropriated R.P.'s funds instead of investing them as represented.

Respondent's course of business to deceive and defraud R.P., including making untrue statements of material fact by invoking non-existent regulators, sham compliance processes and fee requirements to extract additional payments in connection with the offer and sale of a security violated § 30-10-301(1)(a), (b), and (c), MCA. Respondent impersonated a legitimate investment firm, developed trust with R.P., and induced him to invest money and provide sensitive personal and financial information in response to fabricated "regulatory reviews" and "compliance holds." Instead of investing his funds as represented, Respondent misappropriated them. This course of conduct-employing a scheme to defraud, making untrue material statements and omissions (including invocation of non-existent regulators and sham compliance processes and fee demands), and engaging in a course of business designed to deceive and defraud R.P. in connection with the offer and sale of a security-violates Mont. Code Ann. § 30-10-

301(1)(a) (device, scheme, or artifice to defraud), § 30-10-301(1)(b) (untrue statement of material fact or omission), and § 30-10-301(1)(c) (acts or practices constituting fraud or deceit).

9. Respondent's fraudulent scheme resulted in personal financial loss to R.P. and is grounds for the Commissioner to require Respondent to make restitution for all losses sustained as a result of Respondent's actions.

FINAL ORDER

THEREFORE, based on the foregoing findings of fact and conclusions of law, it is hereby ORDERED that:

1. Respondent has violated §§ 30-10-201, 30-10-301 MCA.
2. Pursuant to § 30-10-305(3)(a), Respondent shall pay a fine of \$20,000 for violating § 30-10-201(3), MCA, plus interest at the statutory rate, against Respondent for violating § 30-10-201(3), MCA. Such fine shall be subordinate to the restitution in the event Respondent is unable to pay the full amount of the fines and restitution.
3. Pursuant to § 30-10-309, MCA, an order requiring Respondent to pay restitution for the total losses to R.P. in the amount of \$955,932.29, together with interest at the statutory rate.
4. Such fine shall be subordinate to the restitution in the event Respondent is unable to pay the full amount of the fines and restitution.

DATED this 11 day of May 2026.



JAMES BROWN

Commissioner of Securities & Insurance,
Office of the Montana State Auditor

CERTIFICATE OF SERVICE

I hereby certify that on May 12th, 2026, I caused a copy of the foregoing *Final Agency Action and Default Order* to be served on the following persons via email with the address that was provided:

Baillie (Bailey) Gifford
VIA EMAIL
support@bailglobalmarket.com

/s/ Jennifer Whalen
Jennifer Whalen
Paralegal

cc: Jack Connors Jack.Connors@mt.gov
Molly VadeVoort Molly.VandeVoort@mt.gov