FICTIONAL SAMPLE · DRAFTED BY DEMANDLETTERHUB FROM A MADE-UP CASE FILE · NOT LEGAL ADVICE

PLEASE VERIFY BEFORE SENDING

Unverified AI draft. Every fact must be checked against the records before use. It is not legal advice. Fill in every [ADD: …] placeholder, set the demand amount, confirm anything marked [VERIFY], and delete this box before sending.

- Total of $723.46 is my addition of the amounts in the costs log, with the premium plan counted as four charges of $24.99 ($99.96). Please check it. The plan may have continued to bill after February 1, 2026, so update through the date of the letter.
- The documents do not directly tie the fraud to the Fernhollow incident. The letter relies on timing and on the data types listed in the breach notice. The credit union denied the $389.95 gift card claim because the merchant showed proof of delivery to an email address. Please confirm that item belongs in the demand.
- The 19.5 logged hours include the 6 hours on November 12, 2025 that are also claimed as unpaid time off ($189.00). Confirm whether the client seeks compensation for any other time, to avoid double counting.
- The reason for the premium identity plan (Fernhollow's offer covers one bureau and has no restoration help) comes only from the client's note. Confirm against the Keystone Identity Services terms. Also confirm whether she enrolled in the free monitoring, since the notice set an enrollment deadline of January 31, 2026.
- The Sterling Row item in the credit union packet is headed "New Account Notice, October 28, 2025" but also describes events on October 29 and December 9, 2025. Obtain the underlying store and credit union letters.
- The privacy policy was saved by the client on June 2, 2025. Confirm that the March 1, 2025 version was the one in effect when she ordered.
- The phishing emails are described only in the client's own note. No samples are in the file.
- Two Virginia legal points are marked [VERIFY] and are not cited to any statute: breach notice and data security duties, and any privacy or consumer protection law that applies.
- Still to be added: date, firm address, delivery method, recipient ZIP, claim or reference number, demand amount, monitoring period, and response deadline.

Whitlow & Brandt PLLC
[ADD: firm street address]
[ADD: city, state ZIP]
[ADD: phone] · [ADD: email]

[ADD: date]

VIA [ADD: delivery method]

Legal Department
Fernhollow Outfitters LLC
2050 Canopy Ridge Drive [privacy_policy_excerpt.pdf p.1]
Ashmont, Virginia [ADD: ZIP]

Re: Demand arising from the data security incident disclosed October 6, 2025. Our client: Marisol Teague. Reference no.: [ADD: claim or reference number, if any]. Unauthorized access period: August 4, 2025 to August 19, 2025

Dear Legal Department:

Introduction

This firm represents Marisol Teague regarding the exposure of her personal and payment information by Fernhollow Outfitters LLC ("Fernhollow"). Please direct all further communication about this matter to our office and not to Ms. Teague.

The breach

Fernhollow's October 6, 2025 Notice of Data Security Incident states that an unauthorized person had access to a legacy order database between August 4, 2025 and August 19, 2025 [breach_notice.pdf p.1]. Fernhollow reports that it discovered unusual activity on a server supporting its online store on August 27, 2025 [breach_notice.pdf p.1]. The notice to Ms. Teague is dated October 6, 2025 [breach_notice.pdf p.1].

According to the notice, the information from Ms. Teague's order included her name, billing and shipping address, email address, phone number, online account password, and her payment card number, expiration date and security code [breach_notice.pdf p.1]. Fernhollow also stated that the information in the legacy order database was not encrypted [breach_notice.pdf p.1].

Ms. Teague placed her order, no. FH-778214, on June 2, 2025 [privacy_policy_excerpt.pdf p.1]. At that time, Fernhollow's posted privacy policy stated that it used "industry-standard safeguards, including encryption of payment card information both in transit and at rest" [privacy_policy_excerpt.pdf p.1]. The policy also stated that Fernhollow keeps payment card information "only as long as needed to complete your transaction and process any return" and does not "store your full card security code after your order is authorized" [privacy_policy_excerpt.pdf p.1]. It further promised that, if it learned of unauthorized access, it would "notify you promptly" [privacy_policy_excerpt.pdf p.1]. Her order confirmation email stated that her payment information was "protected by bank-level encryption" [privacy_policy_excerpt.pdf p.1].

Harm to our client

The events below followed the exposure of Ms. Teague's information, in date order.

- On September 13, 2025, two transactions posted to Ms. Teague's credit card: $612.40 at an online electronics merchant and $389.95 at a gift card merchant. On September 14, 2025, a

further attempted charge of $1,140.00 at an online travel merchant was declined [fraud_and_credit_records.pdf p.1].

- The credit union issued a fraud alert on September 14, 2025 and replaced her card on September 15, 2025 [fraud_and_credit_records.pdf p.1]. She spent 2.0 hours on calls with the credit union on September 14 and 1.5 hours updating her card on automatic payments on September 16 [costs_and_time_log.pdf p.1].
- On October 6, 2025, Ms. Teague read Fernhollow's notice and called its incident line, which took 1.0 hour [costs_and_time_log.pdf p.1].
- The credit union credited the $612.40 claim on October 21, 2025. It denied the $389.95 claim in a letter dated November 3, 2025, because the merchant provided proof of delivery of a digital gift card to an email address [fraud_and_credit_records.pdf p.1].
- On October 26, 2025, a Sterling Row Home Goods store credit account was opened in Ms. Teague's name, using her name and address, and $1,876.33 was charged the same day [fraud_and_credit_records.pdf p.1]. She reported the account as fraud on October 29, 2025, after 2.5 hours on calls with the store's fraud team [fraud_and_credit_records.pdf p.1; costs_and_time_log.pdf p.1]. In a letter dated December 9, 2025, the store confirmed that it closed the account as fraudulent and that she owes nothing [fraud_and_credit_records.pdf p.1].
- On October 30, 2025, she filed Brierfield Police Department report no. BPD-25-11873 and placed security freezes with all three national credit bureaus. Confirmations arrived between November 4 and November 7, 2025 [fraud_and_credit_records.pdf p.1]. That day's work took 3.0 hours [costs_and_time_log.pdf p.1].
- On November 12, 2025, she took 6 hours of unpaid time off work to meet with the police and the credit union [costs_and_time_log.pdf p.1].
- Her November 20, 2025 credit report showed a hard inquiry from Sterling Row Home Goods dated October 26, 2025 that she did not authorize. She filed a dispute on November 21, 2025, and the inquiry was removed on January 8, 2026 [fraud_and_credit_records.pdf p.1].
- In total, Ms. Teague logged 19.5 hours dealing with these events through January 8, 2026 [costs_and_time_log.pdf p.1].
- She reports that she changed the password on every online account that used the same email address, and that she still receives several phishing emails a week that reference her Fernhollow orders [costs_and_time_log.pdf p.1].

Ms. Teague's documented out-of-pocket losses are as follows. The $612.40 charge was credited back, and the Sterling Row balance is not owed, so neither is included.

Item	Date	Amount	Source
Gift card charge not reimbursed by credit union	September 13, 2025	$389.95	[costs_and_time_log.pdf p.1; fraud_and_credit_records.pdf p.1]
Notary fee, identity theft affidavit	October 30, 2025	$15.00	[costs_and_time_log.pdf p.1]

Item	Date	Amount	Source
Certified mail to Sterling Row Home Goods and two bureaus	October 31, 2025	$29.55	[costs_and_time_log.pdf p.1]
Premium identity protection plan, first month	November 1, 2025	$24.99	[costs_and_time_log.pdf p.1]
Unpaid time off work, 6 hours at $31.50	November 12, 2025	$189.00	[costs_and_time_log.pdf p.1]
Premium identity protection plan	December 1, 2025	$24.99	[costs_and_time_log.pdf p.1]
Premium identity protection plan	January 1, 2026	$24.99	[costs_and_time_log.pdf p.1]
Premium identity protection plan	February 1, 2026	$24.99	[costs_and_time_log.pdf p.1]
Premium identity protection plan, charges after February 1, 2026	[ADD: dates]	[ADD: amount]	[ADD: source]

Total (as read from the bills): $723.46

Ms. Teague bought the premium plan because the free monitoring Fernhollow offered covers only one credit bureau and does not include identity restoration help [costs_and_time_log.pdf p.1]. Fernhollow offered monitoring through January 31, 2027 [breach_notice.pdf p.1].

Legal basis

Fernhollow collected Ms. Teague's payment and account information and held it in a database that, by its own account, was not encrypted [breach_notice.pdf p.1]. Its published policy represented that payment card information was encrypted at rest, was kept only as long as needed, and did not include a stored security code [privacy_policy_excerpt.pdf p.1]. Fernhollow's notice describes a different situation. Fernhollow also told customers it would notify them promptly of unauthorized access [privacy_policy_excerpt.pdf p.1]. Its notice to Ms. Teague is dated October 6, 2025, after the August 27, 2025 discovery date it reports and after the September 13, 2025 fraudulent charges on her card [breach_notice.pdf p.1; fraud_and_credit_records.pdf p.1].

We believe these facts support claims against Fernhollow under Virginia law, including for failure to safeguard customer information and failure to give timely notice. [VERIFY: Virginia rule on data breach notice and data security duties] [VERIFY: Virginia privacy or consumer protection law that may apply]

Demand

On behalf of Ms. Teague, we demand that Fernhollow:

- Pay our client [ADD: demand amount], including reimbursement of the documented losses above and any further documented costs through the date of payment.

- Provide credit monitoring and identity restoration services for [ADD: period], covering all three national credit bureaus.
- Explain in writing exactly what data of Ms. Teague's was taken or accessed, whether it was copied or removed from Fernhollow's systems, and what steps Fernhollow has taken to secure its systems and customer data.
- Preserve all records about the incident, including server and access logs, the investigation and outside security firm's findings, records of the legacy order database and its retention, and all communications with customers and law enforcement about the incident.

Please respond in writing by [ADD: response deadline]. If we do not receive a satisfactory response, Ms. Teague will consider all remedies available to her. Nothing in this letter waives any of her rights or remedies, all of which are reserved.

Sincerely,

Catherine M. Whitlow
Whitlow & Brandt PLLC