THE CONSUMER SURVIVAL PLAYBOOK

OMNICHANNEL ESCALATION & UDAAP EXPOSURE ARCHITECTURE

Strategist: Charles W. Kinslow IV, J.D., C.P.A.

EXECUTIVE SUMMARY: NAVIGATING AUTOMATED DISPUTES

I have struggled immensely with whether or not to actually publish this. For weeks, I have debated the ethics of releasing this information. Buy Now, Pay Later platforms process tens of billions of dollars annually, providing a genuinely necessary financial lifeline for individuals who are just trying to afford basic necessities. I am deeply conflicted about putting a strain on their operational resources, because I know that when a company takes a financial hit, it is the rank-and-file employees who suffer the consequences of layoffs, not the executives.

However, my conscience will no longer allow me to stay silent. Everyday people are having their limited funds trapped by automated systems they do not understand. What follows is a factual, step-by-step manual for consumers to reclaim their funds under the Fair Credit Billing Act, using the exact documented steps, dates, and regulatory escalations I recently used to force a resolution from two major technology companies (Affirm and Anthropic).

PART I: THE PRECEDENT – UNMASKING "CUSTOMER SUPPORT"

Before dealing with tech subscriptions or loan platforms, you must understand that what companies call "software anomalies" are often deliberate hurdles designed to induce dispute fatigue, and "customer support" is frequently a facade.

The Evolve Bank Breach & The 86-Minute Sham

In mid-2024, Evolve Bank & Trust—Affirm's card partner—suffered a massive ransomware breach leaking SSNs and bank accounts. Leveraging this systemic vulnerability, a malicious actor hacked my Shop account on July 7, 2026, and used my Affirm credit facility to fraudulently purchase $104.63 of merchandise from Perfume Empire (Order PE270138). The package was routed to a fraudulent address (81 Keever Ct, San Jose, CA), directly contradicting my verified, lifetime billing footprint exclusively in Monroe, Louisiana (1002 Park Ave).

I immediately initiated phone calls to Affirm customer service. I was routed to 5 different departments, forced to recite the exact same facts to every new representative, only to be told that the reason the prior department transferred me could not actually be addressed by the new department. They refused an administrative freeze, placing my linked Regions Bank LifeGreen eAccess account (*4082) at risk of a $60 working capital liquidity trap. A representative told me to "rest assured" that I would not be charged.

That was a lie. Affirm opened a fraud investigation via email on July 9 at 11:47 AM (Agent Jason D.), promising a 30-day review. Exactly **86 minutes later**, at 1:13 PM, they sent a subsequent email summarily closing the investigation and holding me liable. An automated algorithm ignored the IP geolocation mismatch, device IDs, and the San Jose drop.

Law Enforcement Intervention & The Executive Confrontation

Automated systems routinely ignore basic consumer statements, so you must shift the legal burden by turning a civil dispute into an active criminal investigation. On July 9, 2026, at 1501 hours, I filed an official Identity Theft Report (Case #2026-00029572) with the Monroe Police Department, handled by Corporal Timothy Yruegas (Badge MPD1125), who was ironically battling his own fintech ID theft dispute with Klarna.

I bypassed the automated dispute loop and tracked down "Scott from Customer Support," identifying him as Scott Williams, VP of Customer Relations. I emailed him directly at his corporate address. I explicitly notified Mr. Williams that I had arranged a three-way phone call between us and Cpl. Yruegas to satisfy their physical report requirement. I cemented this threat by sending the actual drafted playbook directly to him on July 17, 2026. When you introduce a documented police report, an active law enforcement officer, and a compiled public playbook to an executive's inbox, the automated denials stop immediately.

The 22-Minute Operational Paradox & The Chen Liability

A highly targeted complaint was submitted strictly to the CFPB. Simultaneously, a formal Complaint and Jury Demand was drafted for the Northern District of California alleging violations of FCRA, TILA (Reg Z), EFTA (Reg E), and the California Unfair Competition Law. In a state of internal panic, Affirm's operational and legal silos collided:

- **5:10 PM:** Affirm's system issued a ping demanding I log into the compromised portal to resolve the account ("Scott from Affirm Support sent you a secure message").
- **5:32 PM:** Andy Chen, Affirm’s Managing Counsel of Litigation, issued a formal Cease and Desist order, threatening legal action if I contacted personnel or managed the account.

Affirm demanded secure portal login exactly 22 minutes before Legal issued a C&D preventing it. Chen later violated his own C&D to initiate post-CFPB contact, mocking my state law school J.D. credentials. I delivered the drafted playbook to him, CC'ing the compliance officers of direct BNPL competitors (Klarna, Sezzle, PayPal, Synchrony). Affirm capitulated.

PART II: BREAKING THE BOT WALL (THE OMNICHANNEL ESCALATION)

Tech vendors intentionally insulate themselves behind automated bots. Here is exactly how a recent $221.98 dispute was forced into manual resolution by exploiting a company's regulatory and financial vulnerabilities.

The Setup: "Booger Two Shoes"

On June 11, 2026, I paid $221.98 for a "Claude Pro" premium subscription from Anthropic PBC using a prior Affirm digital card. Due to severe frustration with Claude's memory degradation, the account had been nuked and a new profile created under the alias *"Booger Two Shoes."* After a third-party hack, Anthropic abruptly suspended my account, downgraded my tier, retained my funds, and restricted all customer support to an automated chatbot.

The Nuclear Targeting Matrix

When the bot ignores you, you must deploy an Omnichannel Escalation. You do not email support; you email the entities that control the company's financial future. I drafted a cold, factual email detailing their deceptive practices and aimed it directly at the apex of their corporate structure:

- **The C-Suite:** Dario Amodei, Daniela Amodei, Tom Brown, Tom, Brian, Jared.
- **The Cap Table:** Yasmin Razavi (Spark Capital) and Luke Muehlhauser (Open Philanthropy).
- **The Leverage (CC Line):** Personnel across Finance, Sales, Marketing, HR, Legal, and Operations at OpenAI and Google; key U.S. legislators including Senators Richard Blumenthal, Bernie Sanders, and Amy Klobuchar; and Department of Defense (DoD) officials.

Weaponizing Live PR & Filed Federal Complaints

The escalation was completely amplified on July 14, 2026. I directly attacked their brand equity by forwarding them live media URLs detailing their active scandals (*"Anthropic's Ethical AI Just Got Caught Snooping"*). More importantly, I attached a finalized, filed **FTC Complaint.pdf** to the email dispatch. I explicitly quoted Danny Kitishian's KLOVER.AI financial analysis regarding their impending IPO: *"Anthropic's vulnerabilities stem from a contradictory corporate identity, profound product management failures, unsustainable token economics... potentially transforming a triumphant trillion-dollar debut into a cautionary tale of valuation overhang."*

To ensure this PR and regulatory failure was exposed at the highest level, I expanded the CC matrix to include the Senate Commerce Committee, Senate Judiciary Committee, and individual lawmakers known for aggressive tech oversight (Sens. Cruz, Booker, Hirono, and Rep. Cori Bush).

The Capitulation

You force them to realize that ignoring a $221.98 refund is not worth exposing their competency failures to lawmakers, the DoD, and competitors right before an IPO. After the deployment of this exact strategy,

Anthropic capitulated. On July 16, 2026, an Anthropic representative named Sabrina bypassed the bot wall, flagged the payment method as fraudulent, and issued a full refund directly to the alias:

"Full refund Booger, here's the docs, we're really sorry."

PART III: SUPPLEMENT - CIVIL CAUSES OF ACTION & REGULATORY GROUNDS

When executing an omnichannel escalation against a financial institution or tech entity, standard customer service complaints are ineffective. The corporate structure will only react to articulated legal liability. The following section outlines the exact statutory architecture and civil causes of action utilized to corner Affirm into a full surrender. By weaponizing their operational failures against federal and state mandates, you bypass arbitration and threaten them with systemic civil exposure.

1. Fair Credit Reporting Act (FCRA) – 15 U.S.C. § 1681s-2(b)

The Violation: Failure to Conduct a "Reasonable Reinvestigation"
The Execution: Under Section 623(b) of the FCRA, once a furnisher of credit information is notified of an identity theft dispute, they are statutorily required to conduct a "reasonable reinvestigation" into the billing error. Affirm violated this standard explicitly when Agent Jason D. initiated an investigation at 11:47 AM and summarily closed it 86 minutes later at 1:13 PM. It is a mathematical impossibility for an investigator to thoroughly review IP address geolocation logs, Canvas browser fingerprint mismatches, and the San Jose, CA delivery anomaly against a Monroe, LA footprint in 86 minutes. This proves their "investigation" is an automated, bad-faith rubber stamp designed to shift liability.

2. Truth in Lending Act (TILA) & Regulation Z – 15 U.S.C. § 1640

The Violation: Non-Compliance with Mandatory Billing Error Procedures
The Execution: Following the Consumer Financial Protection Bureau's (CFPB) May 2024 interpretive rule, BNPL providers like Affirm are legally classified as credit card issuers under TILA and Regulation Z. They are no longer exempt from traditional credit protection standards. Affirm breached TILA by failing to halt collection efforts during an active fraud review, refusing to issue an administrative freeze when the transaction was pending, and utilizing algorithmic denials instead of the mandated good-faith billing error resolution procedures.

3. Electronic Fund Transfer Act (EFTA) & Regulation E – 15 U.S.C. § 1693g

The Violation: Imposing Liability for Unauthorized Transfers
The Execution: Under EFTA and Regulation E, the burden of proving that an electronic transfer was authorized rests entirely on the financial institution. Affirm wrongfully placed the burden of proof on the consumer to disprove the $104.63 Perfume Empire charge. Furthermore, their refusal to freeze the compromised account placed my connected Regions Bank LifeGreen eAccess account (*4082) at immediate risk of automated drafts, initiating a $60 working capital liquidity trap. Their failure to protect linked external assets from unauthorized drafts triggers severe EFTA liability.

4. California Unfair Competition Law (UCL) – Cal. Bus. & Prof. Code § 17200

The Violation: Unfair, Deceptive, and Abusive Acts or Practices (UDAAP)
The Execution: Because Affirm is headquartered in San Francisco, California, they are subject to the California UCL, which prohibits any unlawful, unfair, or fraudulent business act or practice. Affirm committed a textbook UDAAP violation by engineering an operational paradox intended to force a consumer default. At 5:10 PM, their automated system demanded that I log into the secure portal to resolve the account status. Exactly 22 minutes later, at 5:32 PM, Managing Counsel of Litigation Andy Chen issued a formal Cease and Desist, threatening legal retaliation if I managed the account. Demanding a consumer utilize a portal while legally threatening them if they do constitutes systemic, deceptive entrapment.

5. Breach of Implied Covenant of Good Faith and Fair Dealing

The Violation: Willful Deprivation of Contractual Benefits
The Execution: Every consumer contract contains an implied covenant that neither party will do anything to destroy the right of the other party to receive the fruits of the contract. Affirm breached this covenant by aggressively marketing their platform as "secure" while systematically deploying front-line representatives trained to deliver false assurances (the "rest assured" lie) and utilizing unmonitored APIs to instantly reject legitimate fraud claims based solely on a merchant's "processed" shipping status. Their internal architecture is designed to frustrate the consumer's contractual right to security.

PART IV: LEGAL FRAMEWORK & OBSTRUCTION EXPOSURE

The following legal memorandum outlines the exact statutory architecture utilized to trap financial institutions that attempt to hide digital footprints or operational timelines during an active identity theft dispute.

```
LEGAL MEMORANDUM
TO: Consumer Record file
DATE: July 16, 2026
SUBJECT: Liability for Financial Institution Obstruction of Justice via Concealment
("Hiding") of Digital Transaction Logs and Fraud Timelines

1. Executive Summary
This memorandum analyzes the legal liabilities of a financial institution (including Buy Now,
Pay Later [BNPL] lenders) that processes a fraudulent transaction, misleads a consumer about
its investigation, and intentionally refuses to disclose (hides) digital logs and security
timelines that prove an internal leak occurred.

While individual customer-service disputes are governed by civil statutes—specifically the
Fair Credit Reporting Act (FCRA) and the Electronic Fund Transfer Act (EFTA)—the intentional
act of hiding or concealing digital files (IP addresses, device identifiers, and breach
audits) to prevent their use in a pending or anticipated criminal investigation constitutes
federal criminal obstruction of justice under 18 U.S.C. § 1512(c)(1) and 18 U.S.C. § 1519.

2. The Factual Scenario
The analysis is based on the following specific sequence of events:
1. Stolen Credentials / Internal Leak: A consumer’s sensitive personal identifying
information (PII) is compromised.
2. Fraudulent Installment Loan: A fraudster uses this compromised data to create an account
and execute an unauthorized transaction.
3. Refusal to Investigate / Misdirection: The financial institution processes the
transaction, ignores clear timelines establishing fraud, and misleads the consumer regarding
its investigatory methods.
4. Hiding the Digital Footprint: The financial institution intentionally refuses to supply,
or actively hides, the digital transaction records that would conclusively prove the
transaction was unauthorized and trace the criminal.

3. Statutory Framework
A. Criminal Obstruction & Concealment Statutes
18 U.S.C. § 1512(c)(1) — Tampering with a Record or Document by Concealment
"Whoever corruptly alters, destroys, mutilates, or conceals a record, document, or other
object, or attempts to do so, with the intent to impair the object's integrity or
availability for use in an official proceeding... shall be fined under this title or
imprisoned not more than 20 years, or both."
Application: If a bank or lender intentionally hides server transaction logs to prevent them
from being used by the victim or law enforcement in a court case, grand jury, or anticipated
police investigation, it meets the definition of felony document concealment.
```

18 U.S.C. § 1519 — Obstruction in Federal/Agency Investigations
"Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States... shall be fined under this title or imprisoned not more than 20 years, or both."
Application: Applies if the institution hides transaction databases or internal data leak audit trails to mislead or impede a federal regulatory agency (such as the CFPB or FTC) or federal investigators.

B. Civil Disclosure & Consumer Rights Mandates
15 U.S.C. § 1681g(e) [FCRA Section 609(e)] — Identity Theft Record Disclosure
Mandate: Requires any business entity that has provided credit or entered into a commercial transaction with an identity thief to provide copies of the application and business transaction records to the victim (or an authorized law enforcement officer) within 30 days of a verified request.

12 C.F.R. § 1005.11(d)(2) [Regulation E] — EFT Dispute Disclosures
Mandate: If a financial institution investigates a dispute and determines that no error occurred, it must provide the consumer with the documents and information it relied upon in making its determination.

4. Analysis: "Hiding" as Criminal Obstruction
To prove that the bank's refusal to provide these logs constitutes the crime of criminal concealment rather than a civil dispute, the prosecution must establish three key elements: [Intentional Act of Concealment] + [Official Proceeding Ongoing/Anticipated] + [Specific Intent to Hinder] = 18 U.S.C. § 1512(c)(1) Violation

5. Controlling Case Law (U.S. Supreme Court)
• Fischer v. United States, 144 S. Ct. 2176 (2024): The Supreme Court ruled that 18 U.S.C. § 1512(c) is strictly limited to conduct that impairs the availability or integrity of physical evidence, records, or documents for use in an official proceeding.
• Yates v. United States, 574 U.S. 258 (2015): The Court confirmed that the term "tangible object" in the context of Sarbanes-Oxley obstruction under § 1519 applies specifically to objects used to record or preserve information.
• Arthur Andersen LLP v. United States, 544 U.S. 696 (2005): The Supreme Court established the "nexus" requirement: the defendant must have corrupt intent and know that their actions will affect a particular, ongoing or anticipated official proceeding.

7. Conclusion and Legal Remedies
While a consumer cannot personally prosecute a bank for criminal obstruction, the consumer can exploit the bank's act of "hiding" documents through three civil and regulatory channels:
1. Filing an FTC/CFPB Complaint for Deceptive Concealment.
2. Civil Spoliation Sanctions via adverse inference instruction.
3. Fraudulent Concealment Claims in state courts.

EVIDENTIARY DOSSIER

FULL TRANSCRIPTIONS OF CORPORATE NEGLIGENCE & LEGAL FILINGS

The following exhibits catalog the raw, transcribed, and undeniable proof of structural failures, legal overreach, and deceptive servicing practices utilized in the complaints to federal regulators.

EXHIBIT A: Chronology of Unauthorized Transaction and Administrative Bad Faith

Phase I: The Breach and Immediate Notification
Focus: Establishing the geographic anomaly and proving immediate mitigation efforts.
• July 7, 2026 | 11:53 AM CDT
o Event: Unauthorized intrusion into Shop account and initiation of Order PE270138 via Affirm credit facility.
o Key Fact: The verified billing profile is anchored exclusively to Monroe, Louisiana. The malicious actor routed the physical shipment to a fraudulent address in San Jose, California.
o Evidence: See Order Confirmation PDF.

• July 7, 2026 | 12:27 PM CDT
o Event: Perfume Empire automated system generates a shipping label via OnTrac (Tracking No: 1LSDCR10011QF38).
o Evidence: See Shipping Confirmation PDF.

• July 7, 2026 | 12:55 PM CDT
o Event: Emergency telephonic notice provided to Affirm Customer Support.
o Key Fact: Affirm frontline agents refuse to place an administrative freeze on the compromised account, citing a "pending" transaction status.
o Evidence: See Screenshots of Mobile Call History.

• July 7, 2026 | 3:36 PM CDT & 4:38 PM CDT
o Event: Formal written cancellation demands transmitted to Perfume Empire via email and merchant contact portal.
o Key Fact: Notice of identity theft and geographic discrepancy provided hours before any physical carrier dispatch could logistically occur.
o Evidence: See Email Thread PDF.

Phase II: The Merchant's Refusal
Focus: Proving the merchant ignored clear evidence of fraud in favor of automated processing.
• July 8, 2026 | 3:23 AM CDT
o Event: Perfume Empire issues automated boilerplate refusal to cancel the order or intercept the package, claiming it has "already processed."
o Evidence: See Email Thread PDF.

Phase III: Affirm’s 86-Minute Sham Investigation
Focus: Juxtaposing Affirm's written promise of a 30-day review with their immediate automated

denial.
• July 9, 2026 | 11:47 AM CDT
o Event: Affirm Customer Care (Agent "Jason") issues formal, written acknowledgment of suspected unauthorized activity.
o Key Fact: Affirm explicitly states the investigation "may take up to 30 days to complete," promises to contact the account holder for additional information, and pauses credit furnishing.
o Evidence: See Affirm Email (thread::tbR0gUxbOMi0c4Vrr1_HC3Q::)

• July 9, 2026 | 12:21 PM CDT & 2:15 PM CDT
o Event: Supplemental telephone calls placed to Affirm to provide tracking metrics for the active investigation file.
o Evidence: See Screenshots of Mobile Call History.

• July 9, 2026 | 1:13 PM CDT (Exactly 86 Minutes Later)
o Event: Affirm's automated system dispatches a final denial, summarily closing the investigation without human review of IP logs, device fingerprints, or geographic anomalies.
o Key Fact: Affirm demands full liability for Loan ID: XQ8M-YX19, in direct violation of the Fair Credit Reporting Act's reasonable reinvestigation standard.
o Evidence: See Affirm Denial Email (thread::tbR0gUxbOMi0c4Vrr1_HC3Q::)

Phase IV: Law Enforcement Intervention
Focus: Formalizing the criminal nature of the event.
• July 10, 2026
o Event: Official Identity Theft and Compromise Report filed with the Monroe Police Department.
o Key Fact: Formal assignment of Case #26-29572.
o Evidence: See Monroe PD Incident Report.

EXHIBIT B: Drafted Federal Complaint (NDCA)

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

CHARLES W. KINSLOW IV,
Plaintiff,
v.
AFFIRM, INC.,
Defendant.

COMPLAINT AND JURY DEMAND

INTRODUCTION
The Fair Credit Reporting Act requires financial institutions to investigate credit disputes in good faith. A hacker compromised Charles W. Kinslow IV's Shop account, used his Affirm Card, and charged $104.63 for perfume shipped to California. Even though Kinslow alerted Affirm and the merchant while the charge was pending, Affirm refused to freeze the account, ignored the California shipping anomaly, and closed the fraud investigation in under 30 minutes. Did Affirm violate its statutory duty to conduct a reasonable reinvestigation?

PARTIES
1. Plaintiff Charles W. Kinslow IV is an individual residing in Monroe, Louisiana. Kinslow is a licensed attorney and certified public accountant.
2. Defendant Affirm, Inc. is a Delaware corporation with its principal place of business at 650 California Street, San Francisco, California 94108.

JURISDICTION AND VENUE
3. This Court has subject-matter jurisdiction over the federal statutory claims under 28 U.S.C. § 1331.
4. This Court has supplemental jurisdiction over the state common law claims under 28 U.S.C. § 1367(a).
5. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Affirm's corporate headquarters is in San Francisco.

FACTUAL ALLEGATIONS
6. On Tuesday, July 7, 2026, at 11:53 AM, an unauthorized third party compromised Kinslow's Shop account and generated a $104.63 virtual loan using Kinslow's Affirm Card to purchase perfume from Perfume Empire.
7. The hacker directed the merchant to ship the items to a drop address in San Jose, California: 81 Keever Ct, San Jose, CA 95127. Kinslow has never resided in California, has never had any items shipped to California, and has a lifetime geographic footprint exclusively in Louisiana.
8. Kinslow immediately noticed the order confirmation email and contacted Affirm by phone at 12:00 PM. Affirm routed Kinslow through five different departments only to state they could not take action while the transaction status was "pending," including refusing to freeze the account.
9. At 12:27 PM on Tuesday, July 7, 2026, Perfume Empire automatically generated an OnTrac

tracking label (No. 1LSDCR10011QF38) but did not hand physical custody of the package to the carrier.
10. At 3:36 PM and 4:38 PM on Tuesday, July 7, 2026, Kinslow sent formal cancellation notices to Perfume Empire's sales email and Shopify online contact form, documenting the hack and instructing them not to ship.
11. At 3:23 AM on Wednesday, July 8, 2026, Perfume Empire replied with a boilerplate email claiming the item had "already shipped" and refusing to make changes or issue a carrier delivery interception.
12. Despite promising to act once the loan status updated from pending, Affirm took no action. Kinslow called Affirm again. It took three separate calls and another multi-department runaround just to get Affirm to open a fraud investigation ticket.
13. Only 30 minutes after opening the investigation ticket, Affirm sent Kinslow an automated email stating the case was closed and that Kinslow was fully responsible for the $104.63 charge because the merchant confirmed delivery to California.
14. On Thursday, July 9, 2026, Kinslow filed a formal police report with the Monroe Police Department, detailing the account compromise and California shipping fraud, and is retrieving the physical copy on Monday.

CAUSES OF ACTION
Count I: Affirm violated the Fair Credit Reporting Act by failing to conduct a reasonable reinvestigation. (15 U.S.C. § 1681s-2(b))
15. Under Section 623(b) of the Fair Credit Reporting Act, Affirm had a duty to conduct a reasonable reinvestigation once notified of the dispute. Affirm willfully breached this duty by rubber-stamping the dispute in 30 minutes without review.

Count II: Affirm violated the Truth in Lending Act by refusing to follow Regulation Z's mandatory billing error procedures. (15 U.S.C. § 1640)
16. Under the Consumer Financial Protection Bureau's May 2024 interpretive rule, Affirm must comply with Regulation Z's billing dispute standards. Affirm breached TILA by failing to halt collection efforts and failing to conduct a good-faith review.

Count III: Affirm violated the Electronic Fund Transfer Act by holding Kinslow liable for unauthorized transfers. (15 U.S.C. § 1693g)
17. Under EFTA and Regulation E, Affirm bears the burden of proving that electronic transfers were authorized. Affirm wrongfully held Kinslow liable for transactions initiated by an unauthorized hacker.

Count IV: Affirm breached the implied covenant of good faith and fair dealing by rubber-stamping Kinslow's dispute.
18. Every contract includes an implied promise of good faith. Affirm breached this covenant by utilizing an automated, rubber-stamp dispute system to deny Kinslow's legitimate fraud claim.

Count V: Affirm acted negligently by failing to protect Kinslow's account from foreseeable cybersecurity threats.
19. Affirm owed Kinslow a duty to safeguard the account. Affirm breached this duty by failing to flag login attempts originating from unrecognized devices located over 700 miles away.

Count VI: Affirm violated state consumer protection laws by deceptively marketing secure payment services. (Cal. Bus. & Prof. Code § 17200)
20. Affirm violated the California Unfair Competition Law by representing to the public that

accounts are secure while systematically using automated processes to deny fraud claims.

DEMAND FOR RELIEF

Charles W. Kinslow IV respectfully requests that the Court enter judgment against Affirm and award the following relief:

• A declaratory judgment declaring the $104.63 loan void, and that Kinslow owes Affirm exactly $0.00;

• An order requiring Affirm to delete all negative credit bureau reporting associated with this account;

• Actual, statutory, and punitive damages for Kinslow's financial losses and credit score damage; and

• Reasonable attorney's fees, court costs, and any other relief the Court deems just.

JURY DEMAND

Charles W. Kinslow IV demands a trial by jury on all claims and issues so triable.

Dated: July 11, 2026

Respectfully submitted,

/s/ Charles W. Kinslow IV

Charles W. Kinslow IV, Pro Se
1002 Park Avenue, Unit 4B
Monroe, LA 71201
chase.kinslow@gmail.com
(501) 707-7779

EXHIBIT C: Statutory Notice of Dispute to Corporate Leadership

TO: max.levchin@affirm.com; mlevchin@affirm.com; resolution@affirm.com
FROM: chase.kinslow@gmail.com
DATE: July 10, 2026
SUBJECT: STATUTORY NOTICE OF DISPUTE AND FRAUD EXPOSURE (Loan ID: XQ8M-YX19)

Dear Mr. Levchin:
I am writing to notify you that Affirm, Inc. is in ongoing violation of federal consumer protection statutes, including the Fair Credit Reporting Act (FCRA) and the Truth in Lending Act (Regulation Z).

On Tuesday, July 7, 2026, an unauthorized hacker compromised my Shop account and used my linked Affirm credit facility to charge $104.63 (Order PE270138). The merchant, Perfume Empire, shipped the item to San Jose, California, despite receiving written notice of the fraud hours before shipment. I reside in Monroe, Louisiana, and have never shipped a package outside of my state.

Your customer care team has acted in profound bad faith. On July 9, 2026, at 11:47 AM, Agent Jason sent me a formal notice (thread::tbR0gUxbOMi0c4Vrr1_HC3Q::) confirming that Affirm suspected unauthorized activity and was initiating a fraud review that would take up to 30 days. Exactly 86 minutes later, at 1:13 PM, your automated system closed the case and rubber-stamped a denial.

A good-faith fraud investigation cannot be completed in 86 minutes. An automated lookup that ignores IP address anomalies, device fingerprint mismatches, and police reports violates your statutory duties.

To avoid litigation, I demand that Affirm immediately execute the following actions:
• Full Reversal of Liability: Permanently extinguish the $104.63 principal balance on Loan ID: XQ8M-YX19 and erase all associated late fees.
• Permanent Credit Protection: Issue an absolute restriction blocking any negative, delinquent, or derogatory remarks regarding this transaction from being transmitted to Experian, Equifax, or TransUnion.
• Production of the Investigative File: Provide a complete copy of the internal electronic file and automated parameters you used to close my dispute within 86 minutes.

I will pick up the certified copy of my police report on Monday, July 13, 2026, and will immediately upload it to parallel regulatory oversight portals, including the CFPB and the Louisiana Attorney General.

If this matter is not resolved within 30 days, I will escalate this file to civil litigation or individual mass arbitration. I will seek actual damages, punitive damages, and all applicable legal costs.

Sincerely,
Charles W. Kinslow IV, J.D., C.P.A.
1002 Park Avenue, Unit 4B

Monroe, LA 71201
chase.kinslow@gmail.com
(501) 707-7779

EXHIBIT D: Transcription of Official Law Enforcement Documentation

Monroe Police Department
Case Number: 2026-00029572
Reported Date: 07/09/2026 15:01
Reporting Officer: Cpl. Timothy Yruegas (MPD1125)
Incident Type: Identity Theft (Statute 14:67.16)

Narrative:
On July 9, 2026 at 1501 hours Charles Kinslow reported an unauthorized purchase through an online application using his identity. I, Cpl. Timothy Yruegas responded to Kinslows residence for contact located at 1002 Forsythe Avenue, apartment 4B.

Arriving on scene I met with Kinslow who explained he had established an account with Affirm which is an online financial application providing installment plans to buyers for merchandise or products. Kinslow stated he was notified on this date a purchase of $104.63 was completed from the store labeled La Vie Est Belle by Lancome on July 7, 2026. The order delivery address was displayed as 81 Keever Ct San Jose, California 95127 along with the order number assigned PE270138. Kinslow denied making or permitting this purchase and furthermore is not familiar with the delivery address posted upon the purchase receipt.

Kinslow stated he began the procedure of disputing the purchase with Affirm however to complete the process he was requested to report this matter to Law Enforcement. Kinslow denied any other known subjects to have his information related to the Affirm account or identification to open any accounts to his knowledge. Kinslow provided all information related to this unauthorized purchase including an installment plan for the merchandise which set forth three remaining payments of $26.16. All information collected from Kinslow was submitted to evidence for any further review.

Considering Kinslow had no information to provide to make known any possibility of a subject obtaining his information or identity within the state of California this matter would be pending investigation by Affirm. Any further information regarding this matter would be included in supplemental reporting.

EXHIBIT E: Source Communications (Affirm, Anthropic, Perfume Empire)

[THE 86-MINUTE SHAM INVESTIGATION]

Date: Thu, Jul 9, 2026 at 11:47 AM
From: Shop Pay - help@shop.affirm.com
To: chase.kinslow@gmail.com
Hello Charles,
Thank you for reaching out to Affirm in regard to shop pay installments! My name is Jason with the Affirm Customer Care Team and I hope this email finds you in good spirits!
I have flagged that there is suspected unauthorized activity on your account and paused credit furnishing on any eligible loans associated with your account while we investigate. Should we need any additional information throughout our review, we'll be sure to reach out. Our investigation may take up to 30 days to complete. Once complete, we'll follow up to provide the outcome.
...
Sincerely,
Jason D.

Date: Thu, Jul 9, 2026 at 1:13 PM (86 minutes later)
From: Shop Pay - help@shop.affirm.com
To: chase.kinslow@gmail.com
Hello Charles,
Thank you for your patience as we investigated your report of unauthorized activity concerning the following loans:
Loan Name: Perfume Empire Loan ID: XQ8M-YX19
After a thorough review, our investigation found that the activity was associated with your account, and the loan remains your responsibility.

[THE 22-MINUTE OPERATIONAL PARADOX]

5:10 PM - Automated Push Notification / Email Received:
"Scott from Affirm Support sent you a secure message." (System mandating login to secure portal for resolution).

5:32 PM - Email Received:
From: Andy Chen, Managing Counsel of Litigation, Affirm
Subject: Cease and Desist
[Legal directive strictly prohibiting contact and threatening legal action if account management is attempted, displaying preview snippet "Please call Affir..." to force engagement through generic channels rather than secure portal].

EXHIBIT F: The Anthropic Extraction & Regulatory Escalation

[THE FTC ANCHOR & MEDIA WEAPONIZATION]

Date: Tue, Jul 14, 2026 at 9:33 AM
From: Chase Kinslow
To: senator@blumenthal.senate.gov, senator@booker.senate.gov, senator@cruz.senate.gov, commerce_democrats@commerce.senate.gov, judiciary_democrats@judiciary-dem.senate.gov, judiciary_republicans@judiciary-rep.senate.gov, judiciary.democrats@mail.house.gov, commerce_republicans@commerce.senate.gov, senator@hirono.senate.gov, cori.bush@mail.house.gov, dario@anthropic.com, daniela@anthropic.com, tom@anthropic.com
Subject: Keep your enemies closer...or simply step back and watch them implode.

https://medium.com/the-deepdive/anthropics-ethical-ai-just-got-caught-snooping-3d6710cb8ac2
https://www.iheart.com/podcast/269-artificial-intelligence-gr-57859414/episode/anthropic-got-caught-secretly-downgrading-338554050/

Charles W. Kinslow IV, J.D., C.P.A.

[Forwarded Message - A $221.98 Lesson in How Not to Run an AI Startup]
[To: Anthropic C-Suite, Spark Capital, Open Philanthropy]
[CC: Google C-Suite, OpenAI C-Suite, DoD Officials (nic@mail.mil, andrea.e.simmons.ctr@mail.mil, louie.r.lopez.civ@mail.mil, christina.l.weber.civ@mail.mil, peter.b.hegseth.secwar@mail.mil), House Judiciary Whistleblower]

"Anthropic’s vulnerabilities stem from a contradictory corporate identity, profound product management failures, unsustainable token economics, catastrophic governmental relations, and highly questionable financial engineering. Together, these strategic mistakes threaten to severely depress the company’s ultimate market capitalization upon entering the public equity markets, potentially transforming a triumphant trillion-dollar debut into a cautionary tale of valuation overhang and market correction." Danny Kitishian, Anthropic IPO: Strategic Pitfalls and Market Capitalization Impact [In-Depth Analysis] [2026], KLOVER.AI, (June 7, 2026), klover.ai.

[Attachment: FTC Complaint.pdf]

[THE CAPITULATION]

Date: Thu, Jul 16, 2026 at 5:08 PM
From: Sabrina from Anthropic
To: chase.kinslow@gmail.com

Hi Booger,
Thanks for reaching out and sincere apologies for the delay here - we’re working hard to restore our typical response times.
I've flagged the payment method as fraudulent to prevent this card from being used for future transactions in our system. I've also processed a refund for the fraudulent charges which may

take about 5-10 business days to fully process.
If you haven't done so already, I strongly recommend contacting your bank to report these unauthorized purchases so they can investigate further and take additional steps to protect your account.
Please let me know if you have any further questions.
Best,
Sabrina

EXHIBIT G: Executive Unmasking & Merchant Refusal

[THE EXECUTIVE UNMASKING - AFFIRM]

Date: Thu, Jul 16, 2026 at 1:37 PM
From: Chase Kinslow
To: scott.williams@affirm.com

I assure you this is a serious matter. See attachments.
Charles W. Kinslow IV, J.D., C.P.A.
[Attachments: Exhibit A - Chronology of Unauthorized Transaction and Administrative Bad Faith.pdf; Police Report .pdf]

Date: Wed, Jul 15, 2026 at 8:06 PM
From: Chase Kinslow
To: scott.williams@affirm.com

I’ve arranged for a three way call with Corporal Timothy Yuergas of the Monroe Police Department, the responding officer to my complaint.
I’m sure he’ll relish your responses as a victim of identity theft in his own right. Talk soon.
Charles W. Kinslow IV, J.D., C.P.A.

[THE MERCHANT REFUSAL - PERFUME EMPIRE]

Date: Tue, Jul 7, 2026 at 3:36 PM
From: Chase Kinslow
To: sales@perfume-empire.com
Please cancel this order immediately. Someone has hacked my account and used my affirm card in making this purchase. I do not live in California and this is the first time I’ve ever heard about your website. I have already spoken with Affirm but would appreciate fast action on your part if possible. Please contact me at (501) 707-7779 at your earliest convenience.

Date: Wed, Jul 8, 2026 at 3:23 AM
From: Perfume Empire
To: chase.kinslow@gmail.com
Thank you for contacting us. We are sorry that your order is already shipped. We received your email after we processed and shipped the order. We are sorry that we are unable to make any changes to the order at this time.

EXHIBIT H: The Playbook Drop to Executive Leadership

Date: Fri, Jul 17, 2026 at 12:01 AM
From: Chase Kinslow
To: "scott williams@affirm.com"
Subject: DRAFT: Consumer Resolution Playbook - Navigating Automated Financial & Tech Disputes

I have struggled immensely with whether or not to actually publish this.

For weeks, I have debated the ethics of releasing this information. Buy Now, Pay Later platforms process tens of billions of dollars annually, providing a genuinely necessary financial lifeline for individuals who are just trying to afford basic necessities. I am deeply conflicted about putting a strain on their operational resources, because I know that when a company takes a financial hit, it is the rank-and-file employees the people just trying to feed their families who suffer the consequences of layoffs, not the executives.

However, my conscience will no longer allow me to stay silent. Everyday people are having their limited funds trapped by automated systems they do not understand. I have to prioritize helping the vulnerable consumer over protecting a corporation's bottom line.

What follows is a factual, step-by-step manual for consumers to reclaim their funds under the Fair Credit Billing Act, using the exact documented steps, dates, and regulatory escalations I recently used to force a resolution from two major technology companies.

Part 1: The Precedent - Unmasking "Customer Support"

Before dealing with tech subscriptions or loan platforms, you must understand that what companies call "software anomalies" are often deliberate hurdles designed to induce dispute fatigue, and "customer support" is frequently a facade.

On July 7, 2026, a malicious actor hacked my Shop account and used my Affirm credit facility to fraudulently purchase $104.63 of merchandise. I immediately initiated phone calls to Affirm customer service. I was routed to 5 different departments, forced to recite the exact same facts to every new representative, only to be told that the reason the prior department transferred me could not actually be addressed by the new department. It was an endless loop of going around and around. During this exhausting process, a representative told me to "rest assured" that I would not be charged.

That was a lie. Affirm opened a fraud investigation via email on July 9 at 12:47 PM. They sent a subsequent email summarily closing the investigation and holding me liable at 2:13 PM. The time lapse for this "thorough review" was exactly 86 minutes.

Automated systems routinely ignore basic consumer statements, so you must shift the legal burden by turning a civil dispute into an active criminal investigation.

• Law Enforcement Intervention: On July 9, 2026, I filed an official Identity Theft Report (Case #2026-00029572) with the Monroe Police Department.
• The Executive Confrontation: I bypassed the automated dispute loop and emailed Affirm

executive Scott Williams directly, presuming he was in fact the "Scott" I had previously interacted with masquerading as customer support within their app.
• The Trap: I explicitly notified Mr. Williams that I had arranged a three-way phone call with Corporal Timothy Yruegas, the responding officer to my complaint. I ensured Affirm knew that Cpl. Yruegas would relish hearing their responses, as the officer had been a victim of identity theft in his own right.

When you introduce a documented police report and an active law enforcement officer to an executive's inbox, the automated denials stop immediately.

Part 2: Breaking the Bot Wall (The Omnichannel Escalation)

Tech vendors intentionally insulate themselves behind automated bots. Here is exactly how a recent $221.98 dispute was forced into manual resolution by exploiting a company's regulatory and financial vulnerabilities.

On June 11, 2026, I paid $221.98 for a "Claude Pro" premium subscription from Anthropic PBC using an Affirm credit facility. After a third-party hack, Anthropic abruptly suspended my account, downgraded my tier, retained my funds, and restricted all customer support to an automated chatbot.

When the bot ignores you, you must deploy an Omnichannel Escalation. You do not email support; you email the entities that control the company's financial future.

• The Targets: I drafted a cold, factual email detailing their deceptive practices and sent it directly to Anthropic's C-Suite executives.
• The Audience: In the CC line, I included high-ranking executives from their direct competitors (OpenAI and Google), military and defense officials, and key U.S. legislators including Senators Blumenthal, Sanders, and Klobuchar.
• The Leverage: AI companies like Anthropic are currently at a major impasse with the government regarding competency issues, and they, like their competitors, are preparing for highly vulnerable Initial Public Offerings (IPOs). In my email to their leadership, I explicitly quoted financial analysis detailing how Anthropic's profound product management failures and unsustainable token economics threaten to severely depress their ultimate market capitalization.

The Result: You force them to realize that ignoring a refund is not worth exposing their competency failures to lawmakers and competitors right before an IPO. After the deployment of this exact strategy, Anthropic capitulated. On July 16, 2026, an Anthropic representative named Sabrina bypassed the bot wall, flagged the payment method as fraudulent, and issued a full $221.98 refund.

Charles W. Kinslow IV, J.D., C.P.A.
https://www.linkedin.com/in/experiencedaccountantlawyer