Your Tech Ally

Case Study: Financial Fraud

Names and identifying information in this case study have been changed.

Uncovering a Four-Year Employee Theft Scheme

A client asked me to check two odd credit card charges by an employee. I uncovered four years of theft.

Within days, I identified 58 confirmed fraudulent charges across bank statements, credit card records, Amazon order histories, and third-party vendor accounts — work that could have taken over a month without AI-assisted analysis. My investigation confirmed $6,000 in definite theft and flagged $9,500 more as likely or possible. It ended two weeks later with a police referral and pending criminal charges.

Deliverables included analysis and tracking of fraud, visual timelines illustrating the pattern of theft, vendor contact spreadsheets, direct merchant outreach for billing corrections and potential refunds, organized documentation packages for attorneys and law enforcement, and cybersecurity hardening.

At a Glance

Investigation duration	2 weeks from initial request to police referral
Statements reviewed	100+ bank and credit card PDFs across 4 years
Transactions analyzed	~1,000 credit card transactions ~7,000 Amazon line items cross-referenced against CC records
Confirmed fraud instances	58 charges
Confirmed losses	~$6,000
Likely / possible losses	~$9,500
Outcome	Grand larceny — criminal charges filed; police referral made

The Challenge

Mr. and Ms. B's executive assistant and bookkeeper, Ms. F, had broad access to their financial accounts for years. She handled oversight of all spending, made bank transactions, paid bills, issued checks to employees, and verified credit card purchases on behalf of Mr. and Ms. B.

So when Mr. and Ms. B learned of two credit card charges that didn't fit normal spending patterns, they asked me to take a look.

That "look" required reconstructing four years of financial activity across multiple credit cards, multiple bank and investment accounts, multiple online merchants, and multiple Amazon accounts; distinguishing Ms. F's personal purchases from legitimate business expenses (both of which she made using accounts with her personal e-mail); and building documentation solid enough to support criminal prosecution.

Case Study: Financial Fraud

Your Tech Ally

The Scope

I analyzed all of Mr. and Ms. Bs' financial information spanning four years. One of their banks couldn't export its data as spreadsheets, so with an AI assist (and meticulous human spot-checking) I extracted every transaction, normalized the data, and cross-referenced it against Amazon order histories totaling nearly 7,000 line items. I was able to match each credit card charge to the exact orders placed and shipped. Done manually, this could have taken weeks. With AI, it took hours.

I categorized each charge as:

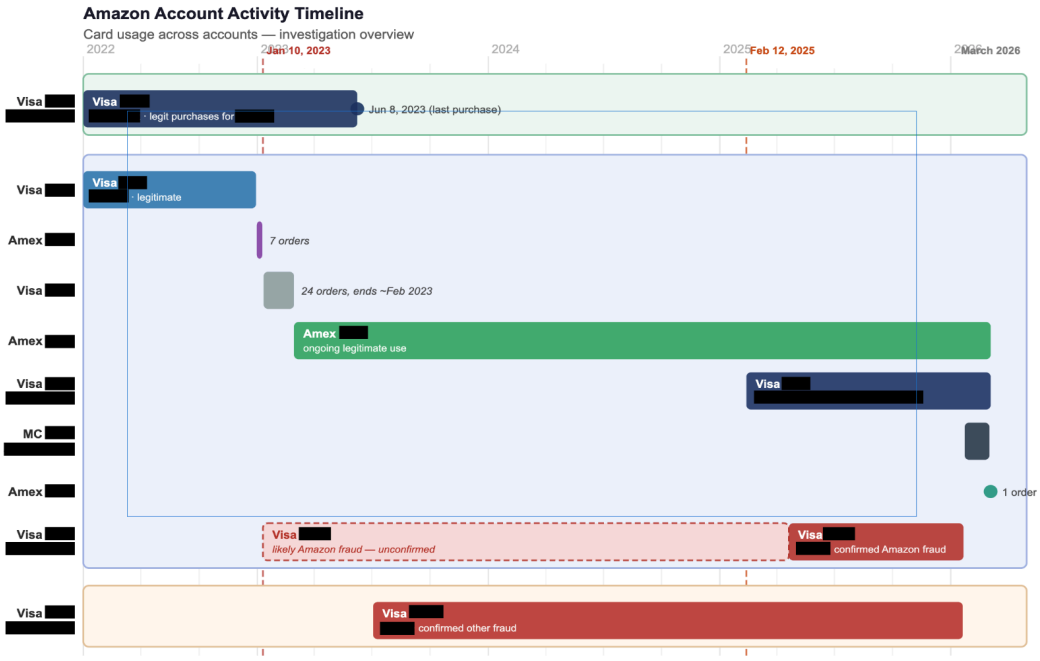
- **Definite fraud** — personal purchases that hadn't been made by Mr. or Ms. B (luxury skincare, clothing, outdoor gear, professional membership dues tied to Ms. F's own outside credentials)
- **Likely fraud** — charges matching Ms. F's known purchasing patterns but pending further confirmation
- **Possible fraud** — unverified charges requiring additional investigation
- **Legitimate** — verified transactions that should be ignored

Key Findings

I uncovered a telling pattern: time after time, Ms. F opened online shopping accounts in her name, entered Mr. B's credit card number and billing address, and shipped purchases to herself. Several times she opened accounts for Mr. or Ms. B, shipped legitimate purchases to them, and then made subsequent fraudulent purchases that she shipped to herself. And I found a years-long pattern of Ms. F's fraudulent purchases on Amazon, in her own account, using Mr. B's card.

Thankfully, I found that the fraudulent activity was limited to just that one credit card. Ms. F had access to all of Mr. and Ms. Bs' financial accounts and could have made illicit electronic transfers, but thorough investigation showed that she had not.

Confirmed fraudulent activity grew approximately 20% year over year across multiple merchants and categories: personal skincare brands, clothing retailers, nutritional supplement resellers, Amazon purchasing (clothing, home goods, gifts, and toys), and even professional membership dues for credentials for Ms. F's own part-time work.



Case Study: Financial Fraud

Your Tech Ally

Complex Recovery

The immediate priorities were uncovering the fraud and preventing future loss. In parallel with discovery and communication about the fraud to vendors, I hardened Mr. and Ms. Bs' digital infrastructure to ensure Ms. F couldn't continue her theft or enact retribution. That meant changing all passwords for their systems: e-mail, computers, network, banks, investments, credit cards, and any online vendors that touched their finances. Since Ms. F had registered many of those vendor accounts using her personal e-mail, it meant updating usernames and removing any methods she might use to recover access to those accounts.

Prevention also meant writing and distributing a technology policy for their employees that included acceptable use and privacy expectations.

Those were the immediate priorities, but there were knock-on effects as well. The sudden firing of such an essential employee left an operational hole in Mr. and Ms. Bs' lives. Suddenly where was no one to handle bookkeeping, purchasing, and bill payments. I ran an analysis of their recurring ACH transactions to ensure they knew which services were paid electronically, and worked to ensure continuity of operations.

Deliverables

Transaction timeline	Charts mapping all cards and account activity
Fraud charge spreadsheet	Dates, amounts, merchant names, and confidence classification
Vendor contact list	Contact information organized for outreach and recovery
Merchant outreach	Direct contact with vendors to flag unauthorized charges
Payment and ACH analysis	Evaluation of all digital transactions, with vendor summaries and payment frequency
Attorney and law enforcement packages	Organized documentation for legal counsel and law enforcement referral
Cybersecurity hardening	Full audit and vulnerability assessment of all accessed accounts; updated credentials and security settings
Technology policy	Written technology use policy for all employees

Tech-Augmented, Human-Supervised

I couldn't have completed the investigation so quickly without AI. That included:

- **Parsing and extracting** structured transaction data from more than 100 PDF statements
- **Cross-referencing** nearly 7,000 Amazon order records against credit card charges to identify exactly which orders were made with which cards
- **Categorizing** hundreds of vendors by type and fraud likelihood
- **Surfacing** behavioral patterns in transaction date data
- **Generating** formatted drafts of deliverables (spreadsheets, timelines, documentation) for attorneys and law enforcement

Case Study: Financial Fraud

Your Tech Ally

AI also helped build the software I used for the analysis. Once I got the thousands of rows of credit card data and Amazon data into their respective spreadsheets, I found they were in completely different structures: different time zones, different date formats, even different groupings of purchases. Sometimes the credit card was charged once but three transactions showed up in Amazon for that purchase. This created real complexity of analysis. AI helped me quickly build highly-complex spreadsheet formulae that definitively matched purchases across the disparate data sets and allowed me to easily categorize the fraud into levels of confidence.

While speed mattered, my point isn't just the speed. It's that AI handled the extraction and pattern recognition so I could focus on the analysis and judgment calls that required human expertise: evaluating patterns to look for intentional fraud, clearly separating circumstantial evidence from what was provable, and building a prosecutable case.

And it's worth mentioning that all client data was handled using privacy-configured AI tools, with settings in place to prevent data retention or training use. And furthermore, all AI involvement was done with the full knowledge and agreement of the clients.

The Human Factor

I brought something to this investigation that the AI could not: empathy. For the Bs, and even for Ms. F.

My early work was conducted through the lens of disproving the pattern of fraud: was there a way to show that this was all an accident? Could it be explained somehow? Even after the pattern was clear, throughout the investigation I found myself correcting the AI: don't assume ill-intent, stick to the facts, and always double check all findings to ensure accuracy.

After all, this investigation had enormous potential for disruption to a person's life. The AI wasn't equipped to hold that nuance or understand the weight of that responsibility. This required empathic, human oversight.

Outcome

The investigation resulted in a referral to law enforcement and expected criminal charges for grand larceny. The evidence package I provided included Mr. and Ms. B's financial exposure, clear evidence of wrongdoing, and (according to the police) more than enough information to bring serious charges.

The access vectors Ms. F used have been closed, and the Bs' potential of future exposure has been dramatically reduced.

Only time will ease the feelings of violation Mr. and Ms. B experienced, but they rest easier knowing Ms. F will answer for her crimes and that their systems are secure.