

Insurance | Sample Cases

The following descriptions highlight a variety of matters for which Vestige has been retained. Each of these cases are real matters that we have worked, but for privacy and confidentiality purposes the identifiable information has been sanitized. These cases are not the entire population of cases matching such criteria, but instead represent a wide sample of the cases we have worked that are specific to Insurance. Should you need additional information, please contact us.

DIGITAL FORENSICS | Document Alteration:

Insurance Company v Insured | Insurance Fraud Matter

Vestige was engaged by a large insurance company in their investigation of the insured's claim. The insured had suffered a catastrophic loss from a fire on a secondary residence. Immediately following the loss the insured presented a detailed list of every item within the secondary residence complete with values, approximate purchase dates, etc. The insured declared that it was simply a recollection of what was in there, created immediately after the event. Due to the level of detail provided in the document the insurance company initially believed that the fire to be arson-related and that the document was created prior to the fire in an effort to maximize the claim. Our analysis indicated that in fact this was not the case and that the document was created after the fire, however, it was based upon records that the insured had been keeping on the computer that existed months to years prior to the fire. Our client, the insurance company, was satisfied with those results and immediately paid the claim.



CYBERSECURITY:

Financial Loss | Cyber Incident Response

A CPA (Certified Public Accountant) was acting as a TPA (Third Party Administrator) for a client business. The CPA was responsible for moving money around within the client's accounts and initiating disbursements. One such day, the CPA's office tried to arrange for a regularly large transfer of money through the bank's website.


Upon entering the credentials and valid numeric key from an RSA Token (2FA | Two Factor Authentication), the bank site indicated a 'down for maintenance' message and to 'try back again'. Over the course of the next several hours the individual from the CPA's office attempted logging in another four times.

Getting towards the end of the day and the possibility of not being able to make the required transfer, the CPA contacted the bank to initiate the transfer manually. During the discussion it was learned that the bank site had NOT been down for maintenance. So the CPA requested a list of transactions - for which there were none.

The next morning the CPA discovered the transfer of the legitimate online disbursements as well as four unauthorized ACH transactions amounting to nearly \$250,000. The CPA quickly made a Loss Claim against their property & casualty insurance for the \$250,000 loss of client money.

The insurance company then engaged Vestige to determine the cause of the financial breach to determine where the breach actually occurred and whether they were going to pay the claim or not.

continued



Our analysis revealed that several days before the unauthorized ACH transaction occurred, one of the CPA firm's employees had received an email with a malware attachment and inadvertently triggered its payload. This resulted in the employee's browser being re-directed to a look-alike web site for the bank (i.e. Pharming) whereby the bad guys (later determined to be from the Ukraine) stole the credentials from the CPA employee when they attempted to log in, the attacker used those credentials to not only login to the legitimate bank site, but also to set up and authorize the four ACH transactions.

Our work for the insurance company proved that the bank's system was NOT the source of the breach, but instead the CPA's firm was the source of the breach. The insurance company paid the claim to the CPA, who then restored the \$250,000 back to the client.



Insurance | Physical Loss Claim

A law firm was broken into one evening and 3 laptops were stolen. The firm filed an insurance claim with their insurer, initially to get back the money to purchase new laptops. Shortly thereafter, it occurred to the firm that the devices contained confidential client data and attorney-client privileged information. The law firm then contacted us at Vestige and through a short interview process we identified that there were some automated tools that ran on the device that we could use to monitor any activity. Within a few hours the thieves turned the devices on and our monitoring picked up their IP address.

We worked with law enforcement (who were involved in the case) to serve a subpoena on the Internet Service Provider, obtained the subscriber information, and the arrest of several individuals was made. Vestige was successfully able to recover and return the devices to the law firm.



Insurance | Arson Investigation

One of the many insurance companies that Vestige works with was investigating a potential arson matter. They recovered a hard drive from a computer that was left in the home during the fire.

Analysis of the hard drive revealed extensive research on the internet including search engine searches and visits to a number of sites and forums with search phrases including *'fire investigations'*, *'beating arson charges'*, and *'accelerants'*. One of the sites that was visited discussed *'the best way to avoid detection'*, which resembled the exact manner in which the fire was caused.

Vestige's digital forensic findings provided some proof that the fire was indeed arson.



Insurance | Fraudulent Claim Analysis

The insurer contacted Vestige because they suspected a fraudulent insurance claim based on the fact that the policy had been put in place three days before the claim was made. The claimant was the owner of an apartment building that had flooded due to frozen water pipes, causing considerable damage.

As evidence of it being a 'good faith' claim, the claimant provided the insurance company with a photo and a video that had been taken on the cell phone of one of the tenants. While the dates and times of the photo and video appeared to be post-dated after the policy inforce date, the insurer had a strong suspicion it wasn't.

Vestige analyzed the photo and the video and discovered evidence that the dates had been manipulated and that the photo had been opened in Adobe Photoshop and the video in Apple Final Cut. We promptly requested the computer that had been used to open the files. The claimant initially refused to turn it over on the basis that the computer had 'crashed'.

Upon a court order compelling the claimant to turn the device over to Vestige, our analysis of the hard drive revealed that it had been disassembled and maliciously destroyed, then re-assembled to make it appear that the damage was happenstance. The data recovery team at Vestige proved that it was intentional and recovered 98% of the data. Analysis of the data proved the files had in fact pre-dated the policy's inforce.

Insurance | Arson Investigation

An insurance company investigating a business fire claim determined that it was not an accident, as evidence of the use of an accelerant was found. The insurer found a damaged digital surveillance system at the business and engaged Vestige to recover and analyze the surveillance system.

Vestige was able to successfully recover video footage. It revealed three individuals entering the business several minutes before the fire broke out. They were in disguise and carrying weed sprayer pumps.

Under Vestige's advice, the insurance company proceeded to contact several local big box building supply stores in the area and compiled all of the transactions that had been conducted involving weed sprayers. Then the insurance company obtained video footage from the store and discovered that it was the business owners who had purchased the sprayers using cash so as not to be traced. However, the business owners failed to take into account they were being recorded on the store surveillance cameras at the cash register.

It was Vestige's ability to recover digital evidence from the original video footage from a no-longer-working surveillance system, analyze, piece together and confirm it was the owners who had committed arson at their own business. The insurance company was very pleased with the evidence Vestige was able to produce to help solve the case.

Insurance Company Panel Counsel | Third Party Risk Mgmt Remediation

Vestige continues to work with a Top 10 Global Insurance carrier on the remediation of Panel Counsel's cybersecurity program worldwide. The carrier, in response to on-going cybersecurity statutes, has implemented a robust Third Party Risk Management (TPRM) program. The Risk Management department for the carrier has determined that all third parties must be 100% in compliance with their requirements. While a large percentage of Panel Counsel can comply, there is a significant portion of firms that are not in compliance and need assistance in getting there. The insurance carrier has a vested interest in making sure these firms remain on their panel and as such is working with Vestige to provide a comprehensive remediation program that Panel Counsel can enroll in. Vestige works with the Panel Counsel and customizes solutions that address a wide range of issues such as: policy & procedure activities (i.e. Written Information Security Program (WISP), Change Management, Incident Response Planning and Disaster Recovery/Business Continuity Planning); technical activities such as implementing vulnerability management, encryption, secure remote access, hardening the Panel Counsel's systems and more. To date we have worked with more than 200 Panel Counsel firms around the world in every time zone and multiple foreign languages.

Vestige Digital Investigations

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

info@VestigeLtd.com | 800.314.4357 | www.VestigeLtd.com

03152022