Review of Business & Finance Studies
Vol. 7, No. 1, 2016, pp. 105-111
ISSN: 2150-3338 (print)
ISSN: 2156-8081 (online)

IBFR
www.theIBFR.com

A REAL WORLD CASE OF IDENTITY THEFT

J. Drew Procaccino, Rider University
Maria H. Sanchez, Rider University

CASE DESCRIPTION

This case examines a real world case of identity theft from start to finish. The case details the victim's experience from the day he was told he had insufficient funds in his bank account and realized that he had been the victim of fraud until the resolution of the fraud. By completing the case, students will learn steps to prevent identity theft and also actions they can take if they do become victims of identity theft. The case was designed to be used in either undergraduate or graduate level classes. It is suitable for an Introduction to Business, an Ethics or a Fraud Detection and Deterrence course. Students typically require one to two hours outside of class to complete the case. The instructor should budget approximately one hour of class time to go over the case in class.

JEL: M40, M19

KEYWORDS: Identity Theft, Fraud

CASE INFORMATION

Local Bank and Checking Account

Jim, a resident of the Northeast, returned home from a week spent out-of-state on vacation. Later the same day, Jim went to the local branch of his bank to cash a personal check. The branch was located across the street from his home and some of the bank tellers knew him as a regular customer. Jim was informed by the bank that his account had insufficient funds to cover the amount of the check. Knowing that there should have been approximately $5,000 in the account, he was a little confused. He thought that perhaps he had made a mistake and had inadvertently tried to cash the check on a different checking account. However, he soon realized that it was the correct account and that he had been the victim of fraud. Jim asked the bank teller how his account had insufficient funds to cash his check and he was told that a check had been recently cashed from that account in the amount of $5,200. Jim then asked for a copy of the check in order to see who had signed it. The bank indicated that the signature resembled the one they had on file for him (apparently in a folder), and although while not a match, the signature on the check was close enough for the teller not to question the validity of the fraudulent check. The thief had a fraudulent driver's license with the victim's name on it and the thief's picture, who was a different race than Jim. The teller who accepted the check from the thief was not one of the tellers who knew Jim.

A representative from the bank informed the victim that the bank had video of the person who had cashed the fraudulent check. Jim was further told that the video was recorded earlier the same day that he had come into the bank upon returning from vacation. He asked the bank to produce the video, but they never did. Jim demanded that the stolen funds be placed back in his account. However, due to the timing of the thief cashing a check and the Jim's attempt to cash another check, the bank had reason to suspect that the 'victim' might be attempting to 'defraud himself', pretending to know nothing about the situation and then claiming he was the victim of fraud. The bank said that they would only place the funds back in the account if local police were satisfied that he had nothing to do with the situation. After being questioned by detectives, Jim agreed to take a polygraph test at taxpayer expense. The test was delayed for weeks, despite the victim

pressing to take it as soon as possible so he could get the funds placed back in his account. Jim demanded to take the test but couldn't get detectives to return his phone calls, and he eventually contacted a supervising officer in the police department. He explained the delay and the lack of response from the detectives. The test was then scheduled to be administered a few days later. Jim passed the test and then took the test a second time to verify the results, which he also passed. (Prior to taking the polygraph, the tester talked with Jim for 10-15 minutes, asking him questions about his family life, parents' occupations, his brothers and sisters, what he does for a living, hobbies, etc., in order to get to know him a little bit. The tester said that he had been administering these tests for about 25 years and he told Jim after the test results were completed that he knew from talking with him that he had nothing to do with the situation.) The police then sent a letter to the head of security of Jim's bank acknowledging the result of the tests. A week later the $5,200 was deposited back into the victim's account, which was about three months since the initial discovery of fraud.

Check Printing

Jim had previously used an Internet-based check printing company for his personal checks in order to save money. He did not know how the thieves gained access to his checking account number, but armed with that number, as well as, presumably, his mother's maiden name, they were able to successfully order the fake checks. These checks were out of sequence from the Jim's actual checks. Also, the style of the fraudulent checks (very generic) was not the same as the checks Jim had previously ordered. The thieves had the checks overnighted to Jim's house so they would know when to wait outside of his house in order to 'intercept' the package, posing as Jim. This way, they could avoid filing a change of address with the check printing company, which may have raised suspicion. (It was unclear if the thieves knew the victim was away on vacation.)

Jim had previously noticed a check for a small amount that had cleared his checking account that was payable to a local branch of a National automotive service center. (He later learned the check was for some automotive parts.) The thieves used the check to test to see if the check would clear the bank. Jim saw that this small check had cleared his account, but he was busy preparing to leave for vacation at the time, and as a result, did not put a hold on the account and look into the matter with his bank. The thieves had apparently verified the current balance in the checking account with the bank, as the small test check was followed up with the $5,200 withdrawal, almost emptying out the account. Subsequently, Jim got a phone call from the garage informing him that he owed for some repairs. He immediately informed the garage that this was a fraudulent transaction, as he had only purchased gas there, but never had repairs done. Jim was informed that the purchase was made by a woman with a child in a Jeep Cherokee. Jim explained that he wasn't married, had no children, and didn't own that vehicle. The garage rep said he had written down the VIN number in case it was fraud. Jim told him to report this information to the local police department, as the detectives are currently working on the case. The garage reported the information and the following day the local police department informed Jim that the VIN number from the Jeep Cherokee matched the VIN of a van registered to a company in Northern New Jersey.

Credit Cards

Fraudulent activity also occurred with Jim's credit cards. The thieves had enough information to re-open two previously closed credit accounts, including one that had been paid off for the final time about five years earlier. The thieves were able to supply enough of Jim's personal information, which presumably included his Social Security number, full name, mother's maiden name, home address, telephone number and account number. Posing as Jim, they used the excuse that the he was going on vacation, and needed checks and credit cards. After the request was made, they waited for delivery outside of Jim's residence, possibly showing fraudulent identification to the driver. This part of the scheme was made easier as Jim lived in a condominium. Had Jim lived in a single-family home, this scenario may have raised some

suspicion. While he was away on vacation, thieves went on a shopping spree in local malls with fraudulently obtain credit cards, buying thousands of dollars of mostly children's clothing. (Jim had no children.)

It was not known how the thieves obtained Jim's personal information necessary to perpetrate the fraud. One of the only hints may be that a few pieces of mail turned out to have been missing during the months leading up to the discovery of fraud, including a credit card statement and a cable television bill. Jim suspected after the fact that the thieves might have been collecting information, specifically account numbers.

Credit Line

Jim also got a phone call from a furniture company which informed him that a piece of furniture that had been backordered had arrived for him. The thieves had applied for credit and purchased a few thousand dollars' worth of bedroom furniture, including waterbeds and dressers. They had previously picked up their items at the store rather than have them shipped to a location. So when the backordered item arrived and the thieves were long gone, the store called the Jim, who subsequently went to the financial institution that had provided the credit for the furniture purchases. He was told by the financial institution that the people who applied for the credit came into the location in person, where they completed the paperwork (and/or possibly were told that they needed to be interviewed regarding their financial situation). Jim inquired as to who was the furniture rep that met with the thieves, and he was told that that individual no longer worked at the store and could not be located. Subsequently, Jim heard that this person had been associated with some other suspicious transactions actions at the same financial institution, but it was not known if this person had anything to do with this situation. Jim asked a rep at the financial institution why someone didn't call to verify his place of employment, and he was told that someone did call, and 'verified' his employment there. However, Jim had never been employed by the company that was called.

Jim, who had earned an associate's degree in Science and Law Enforcement, played detective, even prior to police involvement, and worked as his own advocate in order to find those responsible. He made a point to go to the various organizations involved in this case in order to speak face-to-face with supervisors, including those at the furniture store, financial company and bank. Jim felt that looking into his case was also good for his psyche, being able to do something and not feel so helpless.

Wrap-up

The thieves had taken money from the victim's checking account (through the fraudulent checks), made purchases using Jim's credit card, run up charges related to car repairs, and used credit in his name to purchase furniture. In all, approximately $15,000 in fraudulent charges was made. In the end, the Jim was able to get back almost all of the stolen funds, including the $5,200 withdrawn from his checking account, as well as the various fraudulent charges made on credit cards (Jim recalled that he did not get back the small amount of the original check the thefts used to 'test' his checking account).

Jim had to straighten out his credit report with the three reporting agencies, providing them with reports from local police. In addition, he requested that his bank, credit card companies, and loan institution report the fraud to the credit reporting agencies, which they did. He also put a fraud alert on his credit with the three agencies. Jim continues to get credit reports to insure that everything is straightened out, and his credit rating has remained high. He was able to get everything resolved within one year, but it cost him many hours making phone calls, going to meetings and writing letters. No one who committed any of the fraudulent activity related to his case was ever identified.

QUESTIONS

1. What could the victim's bank have done differently that could have potentially stopped or limited the fraudulent activity?

2. After the fraudulent activity had been discovered, Jim met with a representative of the check printing company regarding policies/controls that the company should consider implementing in order to help identify fraud in the future. What changes would you recommend to the company?

3. What could the furniture store have done differently that could have potentially stopped or limited the fraudulent activity?

4. What could the credit card company have done differently that could have potentially stopped or limited the fraudulent activity?

5. Is there anything the victim could have done *prior* to the fraudulent activity that could have helped to *prevent* this fraud?

6. Is there anything else the victim could have done *after* the fraudulent activity that could have minimized the fraud?

A REAL WORLD CASE OF IDENTITY THEFT

TEACHING NOTES

J. Drew Procaccino, Rider University
Maria H. Sanchez, Rider University

CASE DESCRIPTION

This case examines a real world case of identity theft from start to finish. The case details the victim's experience from the day he was told he had insufficient funds in his bank account and he realized that he had been the victim of fraud until the resolution of the fraud. By completing the case, students will learn steps to prevent identity theft and also actions they can take if they do become victims of identity theft. The case was designed to be used in either undergraduate or graduate level classes. It is suitable for an Introduction to Business, an Ethics or a Fraud Detection and Deterrence course. Students typically require one to two hours outside of class to complete the case. The instructor should budget approximately one hour of class time to go over the case in class.

GENERAL COMMENTS

This case is based on an actual identity theft. Names and minor details have been changed to preserve anonymity. By completing this real world case study, students can go beyond textbook learning. It gives them a chance to see how easy it is for identity theft to take place in the real world. The case should help students develop both written and oral communication skills. This case is appropriate for an Ethics, Introduction to Business or a Fraud Detection and Deterrence course, and it can be used at either the undergraduate or graduate level.

The authors assign the case as an individual assignment, allow approximately one week for the students to complete the case, and spend one class period discussing the solutions on the day the case questions are due. We have found that students find the case to be interesting and informative, and students almost always note to us that upon completion of the case, they plan to be more diligent in protecting their own identity.

QUESTIONS

Question 1: What could the victim's bank have done differently that could have potentially stopped or limited the fraudulent activity?

Solution 1: The bank should have procedures in place to flag unusual transactions. These include asking for two forms of identification or providing answers to security questions for transactions over a certain dollar threshold. In addition, the bank could have a copy of the account holder's driver's license on file and use it to compare to the customer attempting a transaction. They should also verify the customer's signature with the one on file. Customers should be notified of any out of sequence checks. The bank should advise customers to notify the bank when the customer will be out of town. Additionally, procedures should be in place to flag instances of an account being accessed in two different geographic locations within a short period of time.

Question 2: After the fraudulent activity had been discovered, Jim met with a representative of the check printing company regarding policies/controls that the company should consider implementing in order to help identify fraud in the future. What changes would you recommend to the company?

Solution 2: When a customer places an order for new checks, the company should verify this order with the customer via an e-mail address held on file, and then ask the customer to provide the next check number

in the sequence. This number should then be compared to the highest check from the last known check order, if applicable. Alternatively, the company should advise the customer via e-mail if a set of newly ordered checks would be out of sequence from the last ordered set. The company should also note if the style/color of the newly ordered checks differs from the previous order. In addition, any request to ship the checks overnight, as opposed a more typical three-to-five day delivery, should be questioned and noted. If the company has any doubts regarding the authenticity of the check order, they could suggest to the customer that they can ship the order to the customer's bank, instead of home address, where they could be picked up after showing proper identification

Question 3: What could the furniture store have done differently that could have potentially stopped or limited the fraudulent activity?

Solution 3: The store should do background checks on employees. When there is an employee who was noted to have suspicious activity, the store should have investigated other transactions with which this employee was involved, and then follow up with customers as necessary. Also, customer pick-up of large items should be noted as a possible indication of fraudulent activity. It should be noted that when the financial institution ran a credit report on Jim, it should have been a red flag that two credit cards had recently been opened.

Question 4: What could the credit card company have done differently that could have potentially stopped or limited the fraudulent activity?

Solution 4: The credit card company should have contacted the customer to confirm the unusual transaction of re-opening closed credit cards. In addition, they should have flagged suspicious/large transactions, and contacted the customer to verify that these were legitimate transactions before allowing the charges to go through.

Question 5: Is there anything the victim could have done *prior* to the fraudulent activity that could have helped to *prevent* this fraud?

Solution 5: Since the victim did not know how his personal information had been compromised and his identity stolen, any of the following measures *might* have help: protect all personal information including Social Security number, account numbers, mother's maiden name, etc.; alert bank and credit card companies when he would be on vacation and where; shred all paper that contains personal information with a cross-cut shredder; continuously monitor bank and credit activity; be on alert for missing mail; consider using a locked mailbox with a key; put mail on hold with the post office while on vacation; order checks directly from the bank and arrange to pick them up at the bank; never give out personal information over the phone; be aware of email "phishing" activity.

Question 6: Is there anything else the victim could have done *after* the fraudulent activity that could have minimized the fraud?

Solution 6: Jim should have immediately reported the fraudulent 'test' check, as well as instructing the credit agencies to put a fraud alert on his file. He should also have considered filing a complaint with the FTC and notifying the Social Security Administration and the Department of Transportation. In addition, he should have immediately changed all passwords on his personal accounts, in particular those associated with any financial institutions. Lastly, he (and the investigating detectives) should have continued to request that the bank provide a copy of the video that presumably captured the thieves.

BIOGRAPHIES

J. Drew Procaccino is an Associate Professor of Information Systems at Rider University. He received his Ph.D. in Information Science & Technology from Drexel University, his MBA from Rider University, and a Bachelor of Science from Rider College, and Bachelor of Science from Ursinus College. His research has focused on identity theft and management of software development projects. He can be contacted at Rider University, 2083 Lawrenceville Rd., Lawrenceville, New Jersey 08648, USA, Email: procaccinod@rider.edu.

Maria H. Sanchez is a Professor of Accounting at Rider University. She received her Ph.D. in Accounting and her MBA from Drexel University and her Bachelor of Science in Accountancy from Villanova University. Her research primarily focuses on fraud detection and deterrence as well as decision maker behavior in accounting and auditing contexts. She can be contacted at Rider University, 2083 Lawrenceville Rd., Lawrenceville, New Jersey 08648, USA. Email: msanchez@rider.edu