Organizing Credit Card Fraud

Jolly (Shuting) Liang

Overview

Though being warned repeatedly of identity theft and credit card fraud, we usually won't really take prudent actions until something eventually happens to ourselves. In the busy daily life, most of us have traded off our identity information and security process for convenience. Being a typical example, my PayPal account got hacked last year and the fraudster kept using my account to buy games online until I eventually terminated my linked credit card account.

My recent activity - Last 7 days (Aug 27, 2015 to Sep 3, 2015)

Archive What's this Payment status glossary

Date		Type	Name/Email	Payment status	Details	Order status/Actions	Gross
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$25.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$25.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$25.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$25.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$25.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$25.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$25.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$25.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$5.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$50.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$5.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$50.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$25.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$100.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$50.00 USD
Sep 2, 2015		PaymentTo	WWW.Steampowered.com	Completed	Details		-$5.00 USD

Figure 1. My PayPal account got hacked in 2015

To help others avoid such a scenario, I would love to analyze how fraud works so that we could get more insight and take more precaution by looking closer at each step. I will present details of the organization and operation by assuming the role of the head of fraudulent organization and my case study will focus on organizing scalable credit card fraud.

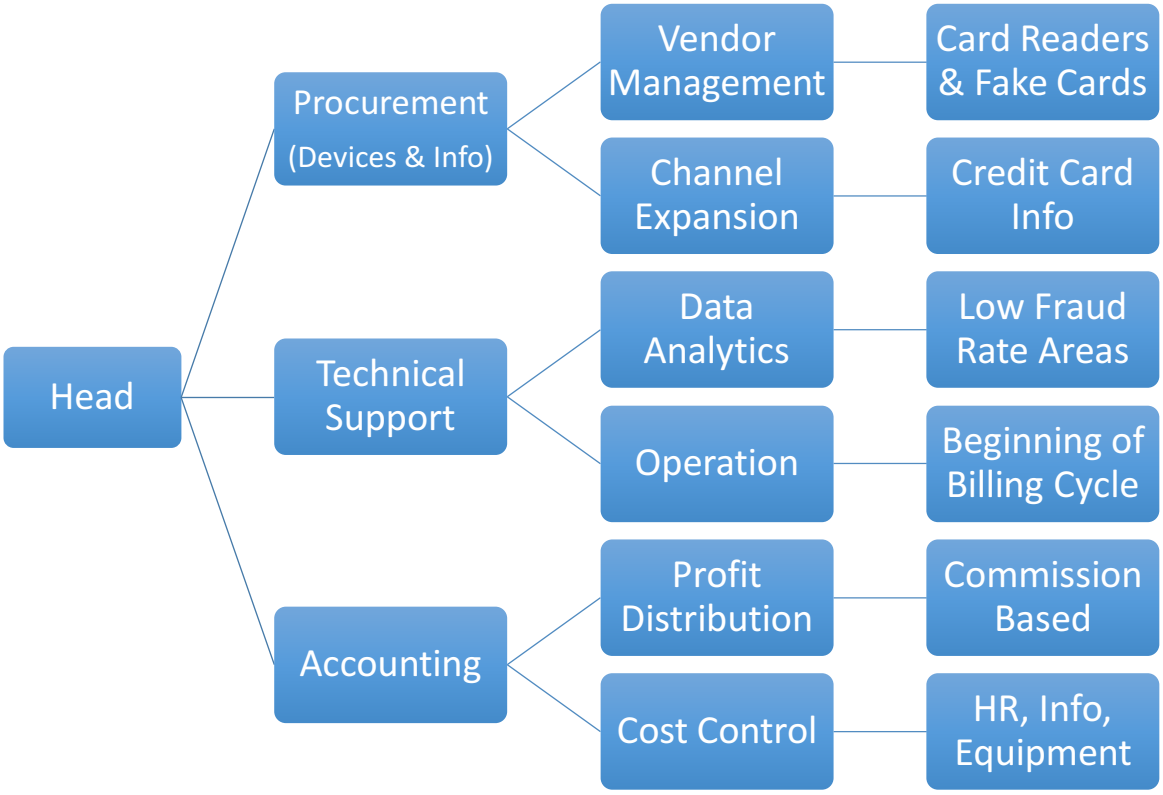

Figure 2. Hierarchical structure of the organizing system

What is Being Organized?

To make sure the implementation could be seamless, long-lasting and scalable, my organizing system would adopt a hierarchical structure and I would divide the management power into 3 teams. Thus as a whole, the fraudulent organization would need to organize: (1) human recourses – 3 teams of professional staff, including the allocation of their individual expertise; (2) physical recourses – devices and equipment, such as contactless card readers (skimmers) and fake cards, etc.; (3) digital recourses and information – credit card information, billing and shipping address information and different datasets

for analytics. The physical resources and digital resources, especially the latter one, should be continually added into collection as the organizing system evolves.

Why is It Being Organized?

An important aspect of this organization depends on centralization of information and clear communication between the team leaders. According to a Sift Science Report, New York is the prime place for fraudsters to mail the stolen purchases, followed by many southern states.[1] Thus orders shipping to these areas might have higher chances of being blocked. Also, according to the secrets exposed by a former credit card thief, there would be less risk to act at the beginning of the billing cycle because many cardholders only check their statement once a month.[2] To reduce the risk, we need to organize the collected datasets to further analyze the safer areas and safer time to take action. Meanwhile, in order to get as much credit card information as we could, we would need to organize our procurement channels – cooperation with restaurant or retailer workers, phishing website owners or cyber-attackers/hackers. To satisfy such an institutional goal of carrying out day-to-day business operations and minimize micro-management, I would need to provide each team with autonomy over their expertise domain.

How Much is It Being Organized?

Precision is essential to the successful function of the fraudulent organizing system. The success rate depends highly on how accurate the credit card information we obtain is and how fast we figure out the billing cycle and take action. Also, how effective the prediction on safe target areas to act on also has important impact on the results. All the above require a fine-grained description of resources, especially of the digital resources. Likewise, each team leader should be fully responsible for his/her team's decision making. Only by

---

[1] Where in America Are the Most Online Fraudsters? (2016, October 25). Retrieved December 2016, from https://priceonomics.com/where-in-america-are-the-most-online-fraudsters/

[2] Secrets of a Former Credit Card Thief. (2011, January 6). Retrieved December 2016, from http://www.creditcards.com/credit-card-news/secrets-former-credit-card-thief-dan-defelippi-1282.php

specifying the accountability could it result in informed decision. To make the organization and implementation scalable, it is also fundamental to design a well-structured schema for the relational database for future expansion. As we will get more and more credit card information, shipping and billing address information, we will need more granular description to better distinguish one from another. Also, as the three teams are in charge of different functions of the organization, there should be different principles at work for each of them. For example, the procurement team should organize the resources by type while the technical team should organize with descriptive statistics and utilize principle that is based on properties derived from the collection as a whole.

When is It Being Organized?

Since fraud action and success depend heavily on information accuracy and prompt retrieval, the organizing system has to place emphasis on generic organization “on the way in” for easier future information retrieval. In short, the organizing system has to make a tradeoff between granularity and abstraction for resource’s description: the procurement team has to elaborate on the model and functionality description of the devices “on the way in”, as well as on the credit card information and expiry information. Otherwise the retrieval for data analytics and operation will not be timely or accurate. However, for the technical support team, who is mainly in charge of data analytics, should organize the resources “on the way out”. It utilizes computational power and algorithm to analyze the collected datasets to yield the ranking of safe target areas and sort the billing cycle information, which actually imposes organization on the available resources “on the way out”. Though all that depends on the generic organization implemented by the procurement team “on the way in”. With regard to the accounting team, the higher revenue the organization brings in, the more can be distributed to expense budget and vice versa. This mutual relationship is actually organizing the financial resources both “on the way in” and “on the way out”. When individual revenue is booked (organized) for commission distribution purpose, the financial resources are organized “on the way in”; however, when the total revenue and cost are calculated together, possible expense budget is determined (organized) “on the way out” based on the previous financial information.

How or by Whom is It Being Organized?

The organizing system as a whole, is organized by the head of the fraudulent organization, that is, I am supposed to take full charge of the organizing system itself. I would personally allocate the management power to each team leader and define their span of control respectively. Since it's in hierarchical structure, it is analogous to how the team leaders should organize their own team. However, the above organization mainly targets human resources. To meet the technical requirement and live up to the accuracy fulfillment, the digital resources should be mainly organized by computer and technical tools under the guide led by people. The procurement team members must make sure all the credit card data collected are completed and would be entered into the database under a meaningful schema, which governs each instance is rigorous enough for future processing by technical support team and future business expansion. Working on the data collected by procurement team, the technical team members should make sure the algorithms and data analytics tools are productive and effective enough to get the desired target areas and action plan information within limited time span.

Where is It Being Organized?

As for the physical resources such as devices and equipment, they should be organized in a "fixed" storeroom before they get allocated to individual skimmer handlers. However, to stay away from police's view, the storeroom should be flexible and get relocated frequently. For the same purpose, all the team members should work remotely using VPN to avoid being traced or located. All the other information and digital resources should be organized and stored "in the cloud" and encrypted. All the data should be backed up and held by at least 2 members. In case one gets caught, at least the daily business operation won't be deterred. On the other hand, all the members should communicate with each other remotely using secret nicknames (anonymous communication utilizing TOR and Darknet[3] systems) to ensure no one knows each other's real identity or location. This is to mitigate the risk of organization breakdown if one member is caught and tries to expose identities of other members.

[3] The Darknet. (n.d.). Retrieved December 2016, from http://theanonymousinternet.tumblr.com/faq

Other Considerations

Given this architectural design of the organization, each team member should have an agile mind and should be granted with discretion to deviate or innovate with respect to the tasks they have been assigned. As the organizing system scales up and the size of resources collection evolves, the hierarchical structure of the organization should expand accordingly over time, same as the encryption system for document storage and internal communication.

Proactive Protection Tips:

- Create complex passwords and set up your calendar to change them periodically.
- Set up calendar to monitor your account activity no less than every week.
- Enroll for custom alerts from your financial institutions to stay informed.[4]
- Utilize encryption tools such as VeraCrypt or Bitlocker to keep your sensitive digital information (such as different accounts and passwords) safe[5].
- Limit entering your sensitive data to secure websites only (One hint: URL begins with “https”) and double think before clicking on any strange hyperlinks, which could be phishing websites.
- Always use a VPN to access public Wi-Fi if you have to send sensitive information back and forth.
- Set up 2 factor authentication utilizing password in combination with another security measure such as email / phone call / SMS or security questions.

---

[4] Cyber Risk Awareness: Preventing PII Theft & Identity Fraud. (2016, October 12). Retrieved December 2016, from https://www.brighttalk.com/webcast/188/221713?utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience7647&utm_campaign=221713&utm_content=2016-10-10

[5] Five Best File Encryption Tools. (2015, February 8). Retrieved December 2016, from http://lifehacker.com/five-best-file-encryption-tools-5677725

CREDIT CARD FRAUD ORGANIZATION

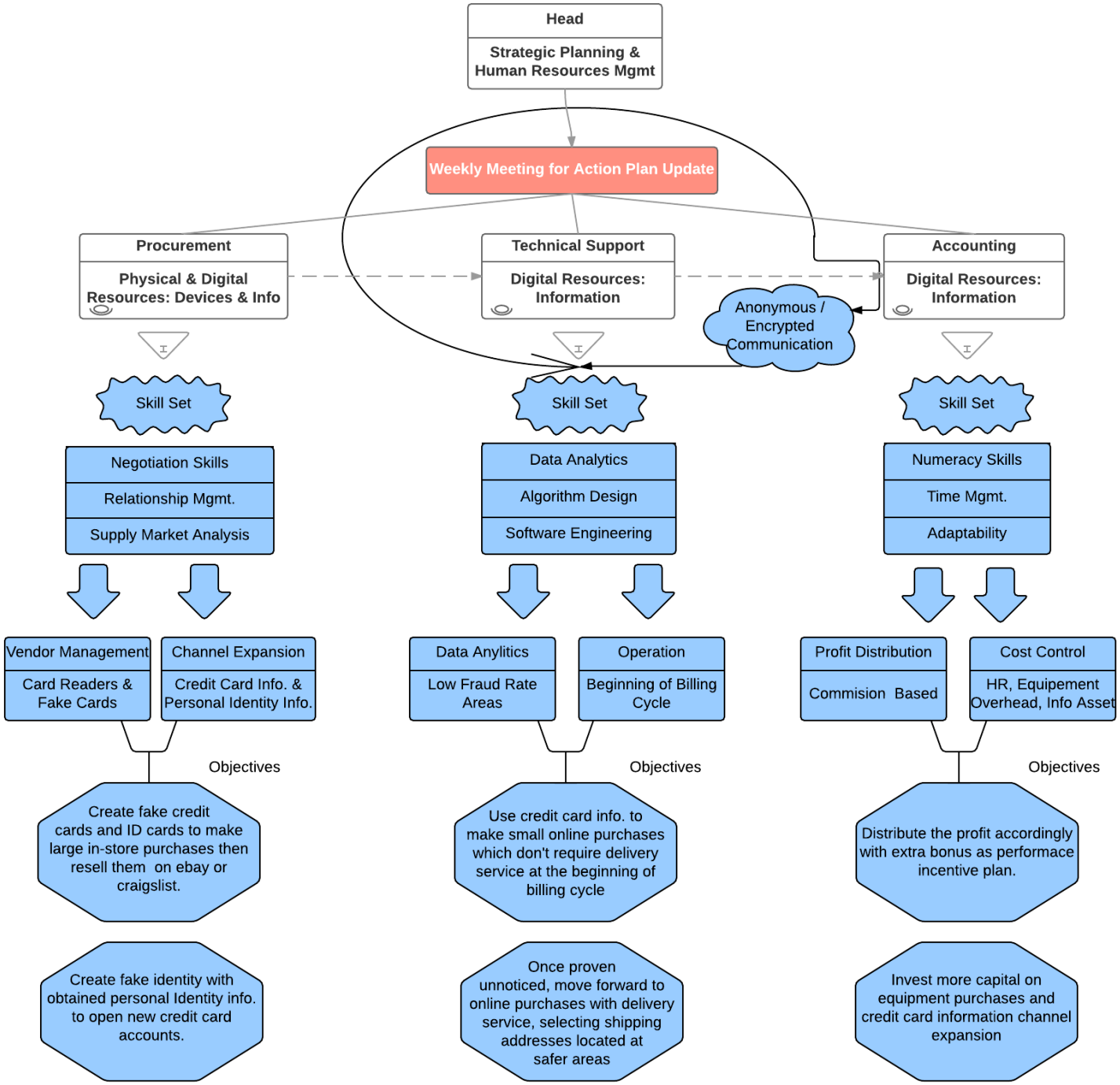

Figure 3. Implementation detail of the whole organizing system