Chapter 87
Credit Card Fraud:
Behind the Scenes

Dan DeFilippi
Independent Researcher, USA

Katina Michael
University of Wollongong, Australia

ABSTRACT

This chapter provides a single person case study of Mr. Dan DeFilippi who was arrested for credit card fraud by the US Secret Service in December 2004. The chapter delves into the psychology of a cybercriminal and the inner workings of credit card fraud. A background context of credit card fraud is presented to frame the primary interview. A section on the identification of issues and controversies with respect to carding is then given. Finally, recommendations are made by the convicted cybercriminal turned key informant on how to decrease the rising incidence of cybercrime. A major finding is that credit card fraud is all too easy to enact and merchants need to conduct better staff training to catch fraudsters early. With increases in global online purchasing, international carding networks are proliferating, making it difficult for law enforcement agencies to be "policing" unauthorized transactions. Big data may well have a role to play in analyzing behaviors that expose cybercrime.

INTRODUCTION

Fraud is about exploiting weaknesses. They could be weaknesses in a system, such as a lack of controls in a company's accounting department or a computer security hole, or a weakness in human thinking such as misplaced trust. A cybercriminal finds a weakness with an expected payout high enough to offset the risk and chooses to become involved in the endeavor. This is very much like a traditional business venture except the outcome is the opposite. A business will profit by providing goods or services that its customers value. Fraud takes value away from its victims and only enriches those committing it.

DOI: 10.4018/978-1-7998-2466-4.ch087

Counterfeit documents rarely need to be perfect. They only need to be good enough to serve their purpose, fooling a system or a person in a given transaction. For example, a counterfeit ID card will be scrutinized more closely by the bouncer at a bar than by a minimum wage cashier at a large department store. Bouncers have incentive to detect fakes since allowing in underage drinkers could have dire consequences for the bar. There is much less incentive to properly train cashiers since fraud makes up a small percentage of retail sales. This is sometimes referred to as the *risk appetite and tolerance* of an organization (Levi, 2008).

Lack of knowledge and training of store staff is by far the biggest weakness exploited when counterfeit or fraudulent documents are utilized by cybercriminals. If the victim does not know the security features of a legitimate document, they will not know how to spot a fake. For example, Visa and MasterCard are the most widely recognized credit card brands. Their dove and globe holograms are well known. A card without one would be very suspicious. However, there are other less known credit card networks such as Discover and American Express. Their security features are not as well recognized which can be exploited. If a counterfeit credit card has an appearance of legitimacy it will be accepted.

BACKGROUND

Dan DeFilippi was a black hat hacker in his teens and early twenties. In college he sold fake IDs, and later committed various scams, including phishing, credit card fraud, and identity theft. He was caught in December 2004. In order to avoid a significant jail sentence, DeFilippi decided to become an informant and work for the secret service for two years, providing training and consulting and helping them understand how hackers and fraudsters think. This chapter has been written through his eyes, his practices and learnings. Cybercriminals do not necessarily have to be perfect at counterfeiting, but they do have to be superior social engineers not to get caught. While most of the cybercrime now occurs remotely over the Internet, DeFilippi exploited the human factor. A lot of the time, he would walk into a large electronics department store with a fake credit card, buy high-end items like laptops, and then proceed to sell them online for a reduced price. He could make thousands of dollars like this in a single week.

In credit card fraud, the expected payout is so much higher than traditional crimes and the risk of being caught is often much lower making it a crime of choice. Banks often write off fraud with little or no investigation until it reaches value thresholds. It is considered a cost of doing business and additional investigation is considered to cost more than it is worth. Banks in Australia, for instance, used to charge about $250 to investigate an illegal transaction, usually passing the cost onto the customer before 2002. Today they usually do not spend effort on investigating such low-value transactions but rather redirect attention on how to uphold their brand. Since about the mid-2000s, banks also have openly shared more security breaches with one another which have acted to aid law enforcement task forces to respond in a timely manner to aid in investigating cybercrime. Yet, local law enforcement continues to struggle with the investigation of electronic fraud due to lack of resources, education, or jurisdictional issues. Fraud cases may span across multiple countries requiring complex cooperation and coordination between law enforcement agencies. A criminal may buy stolen credit cards from someone living on another continent, use them to purchase goods online in state 1, have the goods shipped to state 2 while living in state 3, with the card stolen from someone in state 4.

Online criminal communities and networks, or the online underground, are often structured similarly to a loose gang. New members (newbies) have to earn the community's trust. Items offered for sale have