



# Shift4<sup>®</sup>

## Secure Payment Processing

---

### **Terrorism and Credit Card Information Theft**

Connecting the Dots

Authored by Dennis M. Lormel

September 2008

## About the author

### **Dennis M. Lormel**

Managing Director

IPSA International, AML Practice

Dennis Lormel joined IPSA in July 2008 as a Managing Director of the Northeast region. In this role, Mr. Lormel focuses on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) issues, fraud and financial crimes affecting IPSA's clients globally.

Mr. Lormel retired from Federal Bureau of Investigations (FBI) in 2003 following 28 years of service as a Special Agent. There, he served as Chief, Financial Crimes Section. During his FBI career, amassed extensive experience directing numerous high-profile investigations particularly in complex, document and labor intensive financial cases. He developed, implemented and directed the FBI's comprehensive terrorist financing initiatives following September 11th attacks which evolved into a formal division of the FBI known as The Terrorist Financing Operations Section.

Mr. Lormel is the recipient of numerous commendations and awards to include the Department of Justice, Criminal Division's Award for Investigative Initiative, and the Central Intelligence Agency's George H. W. Bush Award for Excellence in Counterterrorism, and is an advisor to the Congressional Task Force on Combating Terrorist Financing.

Dennis Lormel was also a former Senior Vice President for a full service corporate security consulting firm where he specialized in AML, terrorist financing, fraud, and financial crimes. He is currently a contributing expert to the Counterterrorism Blog.

## Executive summary

Credit card information theft and fraud has increased at a steady pace over the last five years. It is an area of vulnerability that has been increasingly exploited. As the problem continues to evolve from physical theft to more widespread use of the Internet and technology to facilitate fraudulent activity, the trend will continue to track upward. While criminals do not have a monopoly on credit card information theft and fraud, credit card exploitation and fraud has become a growth industry for terrorists. There is no empirical statistical data establishing the nexus between credit card exploitation and terrorism, but there are ample anecdotal case studies demonstrating how extensively terrorists rely on credit card information in furtherance of their heinous activities. Two of these cases are presented in this white paper.

Compliance methodologies, as well as detective and preventive measures must be developed, implemented, and perfected in order to prevent credit card information theft and fraud. This underscores the importance of information security technology, risk recognition, and fraud prevention. As information security technology and protection of credit card information becomes more sophisticated and fraud prevention mechanisms evolve and improve, we ensure that our National Security is better safeguarded from the threat of terrorism.

## Introduction

In assessing the magnitude of the credit card information theft and fraud problem, it is essential to understand who and what we are dealing with. Who is the enemy and what is the threat they pose? In the post 9/11 world, this is an increasingly vexing question. With that context in mind, the enemy can be characterized in two broad categories, terrorists and criminals. Terrorists are motivated by ideology

and present a threat to National Security. Criminals are motivated by greed, in the form of profit and/or power, and represent a threat to the Economy.

“Economic Jihad” is the term terrorists refer to for raising and using funds, recruitment, and exploiting propaganda. The four essential ingredients of a successful terrorist organization are recruitment, motivation, funding, and sanctuary. Terrorist groups require financial support in order to achieve their goals. They must have effective financial infrastructures to include: sources of funding, the means of laundering funds, and the availability of funding. It should be noted that terrorist organizations have had many years to perfect their methodologies. This places us at a distinct disadvantage. Credit card information theft and fraud represents a lucrative funding stream for terrorists and consequently poses a serious threat to our National Security.

Everyone with responsibility for safeguarding credit card information and preventing credit card fraud must understand that they are engaged in the financial or economic component of the war on terrorism. As such, they are involved in fighting “Economic Jihad.” The reality is that most individuals in this space will probably never deal with terrorists. However, it is possible they will, especially in view of the fact that terrorists are regularly exploiting credit card vulnerabilities. In this regard, it is incumbent on everyone to be vigilant.

## Background

Terrorist operations, including terrorist attacks, require financing. Financing a terrorist group requires significant funding; however, financing a terrorist attack usually does not require significant funds. Every dollar we deny terrorists

from raising diminishes their ability to operate, and to attack us at home and abroad.

A challenge we confront in developing and maintaining viable detective and preventative capabilities is the fact that terrorist groups are learning organizations. They learn from their own history and experience. They also learn from the experience of other groups, both criminal and terrorist. Knowledge and learning are important. The Internet serves as a vital learning and facilitation tool. Terrorist groups assess their own vulnerabilities and adapt new methodologies to offset such vulnerabilities. In addition, they continuously adapt to exploit systemic weaknesses and develop opportunities to tap into new, as well as existing, funding sources. This adaptability factor is an important consideration when monitoring and assessing systemic risk.

From the funding perspective, the second step, planning is critically important. During the planning phase, terrorists determine how much money will be needed to carry out the attack. They also determine the sources of the funds and how the money will flow to the operatives responsible for carrying out the attack. For example, the 9/11 attacks were totally funded by Al-Qaeda. Khalid Sheikh Mohammad, mastermind of the 9/11 attacks, approved funding and was responsible for forwarding funds, through facilitators in the United Arab Emirates and Germany, to the 19 hijackers.

Areas of vulnerability regarding terrorism should be assessed from two domains. First is the vulnerability to society. Terrorists are adept at identifying and exploiting systemic weaknesses. They are astute at understanding risk recognition. In addition, terrorists are extremely adaptable. In the U.S. we enjoy an open and free society. Our openness and freedom offer significant opportunities

for terrorists. This is true both in terms of the threat of a terrorist attack and the threat terrorists pose to exploiting our financial vulnerabilities to include financial institutions and all businesses responsible for credit card information security. The second domain we should assess is the vulnerability to terrorists. The two most important vulnerabilities to terrorists are communications and finance. To better ensure our National Security, we must continue to develop proactive and innovative mechanisms to exploit terrorists' vulnerabilities to communication and finance.

### **Summary**

Business and financial sector training seldom provides specific sessions dedicated to terrorist financing. In most instances where terrorist financing is discussed, it is in a basic and generic context. There is nothing basic or generic about understanding the full gamut of terrorist financing.

For those responsible for credit card information security, the focus should be on the source of funds. Credit card information is vulnerable to theft by hacking, phishing, skimming, and a variety of methods. Once compromised by terrorists, credit card information will be used to generate funding to support terrorist activity. The focus for credit card fraud should be placed on both the source and availability or distribution of funds. The credit card serves as the mechanism for the source and distribution of funds.

Training leads to understanding. Understanding leads to meaningful and consistent strategies. Meaningful and consistent strategies deny terrorists funding. Denying terrorists funding limits their ability to strike and successfully carry out devastating attacks.

## Understanding and disrupting terrorist financing

To achieve a meaningful and consistent impact in disrupting terrorist financing there must be a better understanding of the multi-dimensional elements involved in the funding process. Understanding begins with training. This holds true for the government, business, and financial sectors. Terrorist financing is usually discussed in a broad and generic context, and therefore, seldom understood. To truly understand terrorist financing it must be presented and assessed in specific terms. Terrorist financing training should focus on factors to include:

### 1. Types of terrorist groups

Terrorist groups possess certain similarities; however, they differ in many ways due to demographics and logistics, to include how and where they operate, raise funds, launder funds, and disperse funds. In addition, each organization possesses different funding requirements in order to operate. Likewise, each organization will vary in how they commit credit card information theft and fraud.

### 2. Funding Capacity

In order to succeed, a terrorist group must have the capacity to raise funds, the means to launder funds, and the availability of funds to operate. In addition, the manner in which funds are generated and used varies from organization to organization because of demographic and logistical considerations. Terrorists use credit cards for both fundraising and operational purposes.

### 3. Mechanisms for fundraising and operations

The two mechanisms used for funding purposes

are the formal and informal financial systems. In certain venues, the economies are more formal, relying on the mainstream banking system. Credit cards are a tool of the formal financial system.

### 4. Individuals and cells

Donors, fundraisers, facilitators, recruiters, conduits, leaders, foot soldiers and suicide bombers; each type of individual possesses specific and unique funding requirements. Terrorist credit card use and exploitation will differ according to the unique requirements of each classification of individual mentioned above. Credit card information theft and fraud will be carried out either as a group or individual activity.

## Types of terrorist groups

The first step in understanding terrorist financing is to differentiate the myriad of terrorist groups. In developing an understanding, you must learn about terrorist groups, the nature of their threat, the scope of their operational reach, and their financial infrastructure. Terrorist groups possess certain similarities; however, they differ in many respects due to demographic and logistical considerations, to include how and where they operate, raise funds, launder funds, and disburse funds. Although the need for funds and the operational goals and funding demands for major terrorist groups like Al-Qaeda, Hezbollah, and Hamas may be similar, the sources of funds, actual operations, and application of funds are vastly different. It is critically important to draw the distinctions in operations and funding requirements between various groups in order to develop and implement group specific strategies that disrupt and diminish their ability to raise, launder, and disburse funds. The successful disruption and diminishment of funding flows adversely impacts terrorist operations, thereby reducing their ability to attack.

How terrorists commit credit card information theft and fraud, as well as how they use credit cards will vary from group to group. Activities of certain groups are group or cell oriented. Other groups will have their operatives commit credit card theft and fraud on an individual level. Some groups will use both group and individual tactics. Certain organizations will be more inclined to commit credit card information theft and fraud, while others rely on other funding sources.

Based on an assessment issued by the FBI on January 11, 2007, in conjunction with Director Robert Mueller's testimony before the Senate Select Committee on Intelligence, the following groups were identified as threats to the U.S:

### **Al-Qaeda**

Since 9/11, Al-Qaeda has gone from operating as a terrorist group, with an organizational structure, to evolving into an ideology aligned with regional terrorist groups, back to a group being reconstituted as an organization. Regardless of the form, as a group or an ideology, Al-Qaeda has been a constant threat to U.S. security. It still seeks to infiltrate operatives into the U.S. to conduct catastrophic attacks.

The genesis of Al-Qaeda has caused changes in the manner it raises and uses funds. In the period around 9/11, Al-Qaeda relied on wealthy donors and charities for much of its funding. As the organization became disrupted and less identifiable due to U.S. government action, pressure was brought to bear on wealthy Middle Eastern donors and charities, especially in Saudi Arabia. This led to greater reliance on criminal activities including credit card information theft and fraud to raise funds. Al-Qaeda operatives commit credit card information theft and fraud more on an individual basis than as a group or cell activity; however, depending on the circumstances, they will commit fraud as a group or cell.

Al-Qaeda's funding needs went from being extremely large as an organization to less demanding as an ideology. The reemergence of an organization will require an increase of organizational funding requirements. Operational activities continually require funding sources. If funds are not available through the group, the operators will have to generate funding through their own devices to include criminal activity.

### **Regional Terrorist Groups aligned with Al-Qaeda**

Since 9/11, regional groups have emerged as a significant

threat. They are more autonomous and in many instances have adopted Osama Bin Laden's ideology. Groups to include Jemaah Islamiyah, Ansar Al-Islam, Moroccan Islamic Combatant Group (GICM), and Salafist Group for Call and Combat (GSPC) are examples of highly dangerous and visible regional groups aligned with Al-Qaeda.

In the pre 9/11 environment and shortly thereafter, these groups received funding from Al-Qaeda. When Al-Qaeda's organizational presence diminished, so did its funding support. These groups rely on their own fundraising mechanisms, to include criminal activity. Much like Al-Qaeda, regional terrorist groups commit credit card information theft and fraud more on an individual than group basis. They will commit frauds as a group or cell when the circumstances warrant it.

### **Homegrown Cells**

The homegrown threat is posed by self-radicalized groups and individuals already living in the U.S. who are inspired, but not led by, Al-Qaeda. These groups pose vastly different threats and capabilities in comparison to Al-Qaeda. For the most part, they have proven to be unsophisticated and operate on a small scale. Many of these individuals have funded themselves through legitimate jobs. Homegrown cells have been less inclined to commit credit card information theft and fraud. In general, their schemes will be less sophisticated. They will commit credit card theft and fraud more on an individual basis, but can conduct group or cell frauds.

### **Shia Extremists**

The most notable Shia terrorist group is Hezbollah.

Hezbollah is centered in Lebanon. A great deal of its funding comes from state sponsors Iran and Syria. In addition, Hezbollah has established a worldwide infrastructure that raises significant amounts of funding through organized criminal activity and questionable business practices.

Almost all terrorist groups operate based on ideology. Hezbollah operates with a sense of ideology, but also with a sense of greed. Most other terrorist organizations do not operate with a sense of greed. Hezbollah also requires considerably more money because of its position in Lebanon and its outreach and marketing as a benefactor to the Lebanese people. In addition to state sponsors and criminal activity, Hezbollah has raised significant funds through donations from the global Lebanese expatriate community.

Although the U.S. has designated Hezbollah a terrorist organization, many countries have not, making it easier for Hezbollah to raise funds in those venues. Because Hezbollah functions like an organized crime family, their criminal activities, which include credit card information theft and fraud, are more likely to be group or cell oriented. Their operatives will seldom act unilaterally.

### **Palestinian Terrorist Groups**

Palestinian terrorist groups include Hamas and Palestinian Islamic Jihad (PIJ). Their activities have emanated from the Palestinian territories and have focused their attention on Israel. Hamas is the most recognizable Palestinian terrorist group, especially since gaining political leadership in Palestine. The U.S. recognizes Hamas as a terrorist organization. As is the situation with Hezbollah, many countries do not, which makes fundraising in those territories viable.

Hamas relies on charities, donations, friendly Arab States and state sponsors for funding. Hamas has been particularly skillful in using charities for fundraising and logistical support for their terrorist activities. Hamas also raises funds through taxation and extortion.

From an organizational standpoint, Hamas has not engaged in a significant level of credit card information theft and fraud. The U.S. and Israel have led an international sanctioning effort against Hamas, which has successfully limited, restricted or denied funding sources through banking channels. This has adversely impacted Hamas' operating capability. Hamas has had to rely on informal financial channels such as bulk cash shipments and couriers to receive funding.

### **Domestic Terrorist Groups**

Domestic terrorist groups are those groups operating strictly within the U.S. They encompass a broad spectrum of groups motivated by a number of political and social issues. These groups include white supremacists, militia/sovereign citizen movements, black separatists, animal rights activists and environmental extremists. Funding sources for these groups usually originate with group members, sympathizers or group generated revenue. Groups generate revenue from front companies, either legitimately or illegitimately. Domestic terrorist groups have engaged in less sophisticated individual and group credit card information theft and fraud schemes.

## Funding capacity

Funding capacity is the ability to raise, move, and disburse funds. Terrorist financing is extremely challenging to identify and deal with. Understanding that varying organizations have unique operational considerations, requiring different financial infrastructures, sets the foundation for understanding and developing methodologies to counter these infrastructures and disrupt the flow of funds.

Terrorist groups require financial support in order to achieve their goals. They must have effective financial infrastructures. In order to succeed, a terrorist group must have the capacity to raise funds, the means to launder funds, and the availability of funds to operate. Terrorist organizations have had many years to perfect their funding methodologies. This has placed anti-terrorist financing efforts in a greater reactive posture. As a result, more proactive and innovative detective measures must be devised and implemented. Strategies must be developed that enable investigators to track funds back to their point of origin and forward to terrorist strike teams. One method of accomplishing this is to identify the means terrorists use to launder funds and then trace the flow of funds back to the source or point of origin and forward through the dissemination process to the terrorist operation and ultimately to the strike team. Strategies and methodologies must also be developed to protect financial information to include credit card information from theft and fraud.

Terrorist fundraising is much different than the funding of terrorist operations. Raising funds from various sources differs greatly from the use of the available funds. As a result, detective and preventive strategies must be modified to specifically focus separately and collectively on the sources and application of funds. In addition, the manner in which funds are generated and used varies from organization to organization due to demographic

and logistical considerations. In simplifying the terrorist financing process, we are dealing with three steps, as delineated above:

1. Sources of funds
2. The means to launder funds
3. The availability of funds

Begin with the means to launder funds. This requires the use of the formal banking system, the informal banking system, non-financial companies and/or instruments such as credit cards. There must be a conduit that filters the source or origination of funds through a bank, non-bank financial entity or non-financial entity, making it available and accessible to the individual terrorist, cell or entity at the point of distribution or use. In the majority of instances, financial institutions serve as the conduit or middle ground between the source and distribution of terrorist funding. In this context, financial institutions must understand that they service two distinct dimensions of terrorist financing. Such specific understanding is essential. In most instances, terrorist financiers are extremely adept at compartmentalizing the fundraising and operational funding dimensions from each other. It is extremely important that financial institutions develop detective methodologies capable of identifying terrorist financing in the two distinct funding dimensions.

The first dimension is fundraising or the source of funds. This entails all fundraising mechanisms ranging from donations, charitable giving, legitimate and illegitimate business activity, to criminal activity. Larger amounts of money will be deposited or transferred in this financial dimension, consistent with the donor or business activity.

The second dimension is the operational dimension, which requires the availability and ultimate disposition of funds.

In this dimension, terrorists will use smaller monetary amounts. In either funding stream, terrorists will take the necessary steps to avoid detection.

Terrorists use credit cards both as fundraising and operational mechanisms. As a fundraising tool, credit card information theft and fraud represents a lucrative funding stream. As an operational mechanism, credit cards are used to support terrorist activities.

The unfortunate reality is, regardless of the level of vigilance and detection, terrorists will always have access to funds; however, the more robust the detective and preventive efforts, the greater the likelihood for disruption. Every disruptive success reduces the operational capability of terrorists. In this vein, one of the primary areas of vulnerability to terrorists is finance. It is critically important that financial and non-financial institutions understand this fact and the vital role they play in the process.

## Mechanisms of fundraising and operations

There are two primary methods of transferring funds, the formal and informal financial systems. The formal system consists of commercial financial institutions. The informal system moves funds by means other than using financial systems. Terrorists are quite adept at avoiding financial detection. They rely on both the formal and informal systems to launder and move funds. The degree one is used in preference of the other depends on a number of factors to include culture, sophistication of the banking system in various parts of the world, accessibility, timing, systemic vulnerabilities, opportunities to exploit the situation, situational considerations, the level of investigative scrutiny, and other factors. Whichever system is used, funds are moved with the intent to avoid the attention and detection of law enforcement, intelligence, and regulatory agencies.

In determining which system to use, in addition to avoiding detection, terrorists must consider the benefits and risks associated with both the formal and informal mechanisms. Each system possesses a series of benefits and risks. Just as financial institutions assess risk and determine their risk appetite, terrorists assess the risks associated with the formal and informal systems and determine the level of risk they are willing to tolerate.

Commercial financial institutions include banks, broker dealers, credit unions, savings and loan associations, casinos, insurance companies, currency exchanges, and other entities. Benefits of using financial institutions include the creation of an aura of legitimacy and reduction of the number of people involved in handling the transaction, which in turn, creates an increase in security resulting in less exposure to theft. A few detriments to consider in using financial institutions include creation of a document trail (financial transactions don't lie), exposure of transactions to individuals outside the terrorist group,

and exposure to prosecution and forfeiture. It should be noted that the terrorists responsible for the 9/11 attacks relied primarily on the formal banking system as the funding mechanism to support their activities.

Credit cards are a tool of the formal financial system. They also represent a significant area of vulnerability easily exploited by groups or individuals in furtherance of terrorist activities. Terrorists are opportunists. They are adept at obtaining credit card information through the formal financial system by a variety of means. This heightens the importance of credit card information security.

Informal methods of physically transferring funds include use of courier and bulk cash shipment through conduits to include airplane, ship, automobile, and mail and freight shipment. The regional terrorist group Jemaah Islamiah received a bulk cash shipment from Al-Qaeda to help fund the Bali bombing, which is describe further in this white paper. Benefits of physically moving funds include no traceable paper trail; no third party, such as a bank official, aware of the transaction; and total control of the movement of the money. The major detriment of moving money in this fashion includes the high risk of loss of the funds for a variety of reasons.

Since 9/11, terrorist financing methodologies have consistently evolved and changed in order to avoid detection. Terrorists and terrorist organizations are extremely adaptable and flexible. They continuously seek to identify systemic weaknesses for opportunities to exploit such vulnerabilities. To operate in western society, terrorists must rely more on formal mechanisms. To operate in less advanced financial venues, such as Afghanistan and Pakistan, more informal mechanisms

are used.

Following 9/11, Al-Qaeda took steps to exploit informal financial structures in the Middle East and Central America, and to use formal facilities on a more limited basis because of the investigative scrutiny and international pressure placed on the formal banking system. However, over time and with the evolution of Al-Qaeda from a group to an ideology and their subsequent reemergence as a group, they have gravitated back to the formal sector, while continuing to exploit informal channels. Al-Qaeda, like all terrorist organizations, will use whichever system facilitates its needs and allows them to avoid detection.

An informal mechanism, which is much safer than physically moving money, is the Alternate Value Transfer System. This is an informal system for money payments within a country or internationally. It is a trust based system that is culturally and ethnically driven. This system has been in existence for centuries. It is known by many names, one of the most common being "hawala." It functions as an underground banking system, operating parallel to the formal banking system. This is a desirable system for terrorists and criminals because of the ease of operation. The system is discreet and reliable. It is extremely difficult and challenging for law enforcement to trace transactions or obtain evidence. An outstanding reference document was published by Interpol, entitled "The Hawala Alternative Remittance System and Its Role in Money Laundering."

The two most significant areas of vulnerability or weakness to terrorists and terrorist organizations are communications and finance. These two areas consistently lead to the disruption and dismantlement of terrorist groups and activities. Although terrorists consistently change their methods of operations and demonstrate adaptability at

avoiding detection, they must communicate, raise, and spend money to function. This is where the government and private sector's efforts must exploit the weaknesses of terrorists.

Terrorist financing investigative strategies should focus on the disruption of funding flows. The optimal situation would be to trace terrorist funds back to the point of origin and forward to the terrorist strike team. The next step would be to take investigative action to disrupt and dismantle the identified funding stream. To accomplish this, investigators have to identify three funding tracks. The first is to identify funding flows between a terrorist network or organization and the point of origin. The second is to identify funding flows from the network or organization to fund operations, to include organizational operations and specific terrorist activities. The third is to identify funding flows from operations to individuals, cells or groups.

## Individuals and cells

Individuals engaged in terrorism should not be viewed in the general sense of being “terrorists.” They are not one dimensional. It is essential to identify them according to their specific roles and functions. They include donors, fundraisers, facilitators, recruiters, conduits, leaders, foot soldiers and suicide bombers. Each type of individual possesses specific and unique funding requirements. Some may deal solely with the sources of funds (fundraising), some may deal solely with the use of funds, and some with both. Cells function in a parallel manner. Entities are facilitation tools and serve as money laundering mechanisms.

Terrorist credit card use and exploitation will differ according to the unique requirements of each classification of individual mentioned above. Credit card information theft and fraud will be carried out either as a group or individual activity, usually in accordance with the operating methodology of the terrorist group associated with the individual operatives or cells.

Terrorist financing is complex and difficult to understand, let alone identify. It cannot be viewed from a generic or all encompassing standpoint. As noted above, a full range of individuals and entities possess terrorist funding requirements. Because of the variety of roles and functions, detective mechanisms must be more focused. In most instances, the various types of individuals and entities will have characteristics unique to them. For example, individuals to include leaders, donors, fundraisers, recruiters, facilitators and operatives (jihadists, martyrs, suicide bombers and others) by virtue of their positions will have differing funding requirements. Likewise, financial institutions, legitimate or illegitimate businesses, charities and other conduits will have varying funding needs. Financial requirements and flows for the full gamut of terrorists and terrorist supporters vary according to factors

to include their role, location and affiliation.

As a result of the multi-dimensional face of terrorism, general characteristics, warning signs or red flags can be helpful, but are limited in identifying terrorist financing. A more robust process of identifying terrorist financing risk is to develop financial profiles for the specific individual and entity functions, as described above. Financial institutions and non-financial institutions should assess which terrorist groups, individuals, and entities they are most likely to encounter, and in what capacity. In so doing, they can more accurately develop reasonable detective mechanisms. For example, terrorist operatives are more likely to deal at the retail level while wealthy donors are more likely to engage in private banking.

## Systemic weaknesses

There are at least 12 areas of systemic weakness that terrorists regularly exploit to raise and move funds. At least five of those areas involve credit card information and fraud. They include:

- Identity Theft and Fraud
- Credit Cards
- Criminal Activity
- Internet
- Cyberfraud

### Identity Theft and Fraud

Identity theft is the unauthorized use of personal identifying information belonging to another individual for the purpose of convincing a third party that the unauthorized user is the person described by that identifying information, in order to obtain something of value. The theft of credit card information is one example of identity theft.

Identity falsification is the use of information that differs from the true identifying information of an individual, for the purpose of disguising the true identity of that individual in order to obtain something of value or to forestall the taking of an official action. Information extracted from the theft of credit card information can be used to establish a false identification.

Identity theft and fraud is rarely the sole objective of a crime. They are almost always employed as a means to commit other crime, be it financially motivated, to avoid apprehension or detection, or some other reason. It is a component of many types of criminal activity.

### Credit Cards

Credit cards are extremely vulnerable to fraud. They are used extensively by terrorists. There has been a proliferation of hacking and theft of credit card information. The Internet not only serves as a learning tool for terrorists but also functions as a mechanism to steal credit card information through hacking, phishing, and other means. In many instances, when terrorist operatives are apprehended, they have multiple identifications and credit cards in a variety of names in their possession.

Terrorists use credit cards for two purposes. They use credit cards as a funding mechanism through credit card fraud. Terrorists have raised many millions of dollars through various schemes. Credit cards are also used by terrorists as an operational mechanism. They use credit cards to support their operational activities.

As mentioned at the outset, there is no empirical statistical data establishing the nexus between credit card exploitation and terrorism. However, there are ample anecdotal case studies demonstrating how extensively terrorists rely on credit card information in furtherance of their heinous activities. Below are two cases involving credit card information theft and fraud that have a nexus to terrorism.

### Pakistani Credit Card Fraud Scheme

In 2002 and 2003, a group of individuals of Pakistani descent operated an elaborate multi-million dollar credit card fraud scheme in the Washington, D.C. area. The group engaged in numerous bust out schemes. Members of the group fraudulently obtained social security numbers, work permits, alien registration numbers, driver's licenses,

---

## TERRORISM AND CREDIT CARD INFORMATION THEFT

permanent resident status, and U.S. citizenship. Armed with these false documents, group members were able to obtain credit cards that they used in a variety of fraud schemes. The group also procured credit cards from other Pakistanis who were leaving the country. Their identities were assumed by group members and used for fraudulent purposes. This practice has been used on a recurring basis by ethnic fraud groups.

In certain schemes the group relied on complicit merchants to run up false credit card charges. In addition, credit card information was obtained either wittingly or unwittingly from merchants. This group was extremely opportunistic and perpetrated a multitude of fraud schemes.

Proceeds from the numerous fraud schemes were wired to Pakistan. Telephone numbers in Pakistan contacted by group members were identifiable with Al-Qaeda operatives.

### **Imam Samudra**

More than any other case study, the case of Imam Samudra underscores the critical importance for credit card information security. Samudra is a member of the Al-Qaeda linked terrorist group Jamaah Islamiah in Indonesia. He was the mastermind behind the Bali nightclub bombings in 2002 and intended to finance the Bali attack through cyberfraud.

Samudra is technologically savvy and a computer expert. While in prison in 2004, he wrote a jailhouse manifesto. It was an autobiography of his jihadist life. The book contained a chapter, entitled "Hacking, Why Not." In it, he urged fellow Muslim radicals to take holy war into cyberspace by attacking U.S. computers. Samudra described America's

computer network as being vulnerable to hacking, credit card fraud, and money laundering. The chapter did not focus on specific techniques. It focused on how to find techniques on the Internet and how to connect with people in chat rooms to perfect hacking and carding skills. It was a course of study for aspiring hackers and carders. Samudra discussed the process of scanning for websites vulnerable to hacking and then went on to discuss the basics of online credit card fraud and money laundering.

One of the concerns posed by Samudra's book was that it could serve as a roadmap leading terrorists to more accomplished hackers and enhancing the vulnerability to the U.S. National Security. In 2004, Indonesian police asserted that Indonesia had more online credit card fraud than any country in the world.

One commonality between both of the above cases is that the terrorists involved were opportunists. A variety of schemes were used. Whatever scheme they could perpetrate would be used during the course of their fraudulent activity.

### **Criminal Activity**

Terrorists have increasingly relied on criminal activity to raise funds. In so doing, terrorists have left themselves more vulnerable to detection. When it comes to criminal activity, terrorists are only limited by their imaginations. They will conduct whatever criminal activity they have the opportunity to exploit. They will measure the risk of being detected and weigh the risk against their potential financial or operational benefit.

Credit card information theft and fraud is a criminal activity. Credit cards are also used to support other

criminal activities. Fraud investigators and compliance specialists should remain constantly vigilant for fraud schemes and criminal activity which could be linked to terrorism. What appears to be nothing more than a criminal activity could actually be a terrorist financing operation.

### **Terrorist Exploitation of the Internet**

Terrorist use the Internet for a variety of purposes to include:

- Psychological warfare
- Propaganda
- Fundraising
- Communications
- Information gathering

The Internet offers anonymity and worldwide access. It is a great recruitment and training tool. In addition, the Internet is a significant fundraising tool. Credit card information is extremely vulnerable to Internet exploitation.

### **Cyberfraud**

Cyberfraud ranges from credit card information theft to money laundering. It has been described as the “new cash cow” for terrorists to finance operations. As mentioned earlier, terrorist groups are learning organizations. They use the Internet as a learning tool to commit cyberfraud. Terrorists routinely go to websites and chat rooms where they can learn from each other how to perfect hacking, carding, and other schemes, as well as how to launder money.

## Characteristics and trends

Terrorist and terrorist financing warning signs are constantly evolving due to changing dynamics in world events, such as the global response to terrorism and the ability of terrorists to adapt to changing dynamics. Like characteristic indicators, warning signs are non-static. For example, in response to the 9/11 terrorist attacks, the U.S. and international community took decisive steps to disrupt and dismantle terrorist groups and their financing. In return, terrorists adapted new methodologies to exploit systemic vulnerabilities. The same cycle was repeated following other significant terrorist activities, such as in the aftermath of the Madrid bombings of March, 2004.

One of the true challenges in dealing with terrorist financing is the recognition of the dynamics of change and understanding that terrorist and terrorist financing methodologies will constantly change to avoid detection. Developing mechanisms to identify emerging trends should be incorporated into the risk analysis process.

Based on a number of factors, including the international response to terrorism, the number of terrorist arrests and deaths, recruitment practices, emergence of younger terrorists, and the regionalization of terrorist groups and affiliations, a new generation of terrorists is taking shape. Individuals committing themselves to jihad tend to be better educated, less experienced, more radical, somewhat autonomous, and resilient. They are more engaged in criminal activities or interact to a greater degree with more traditional criminal groups. This new breed is proficient in the exploitation and use of false identification documents, as well as obtaining credit card information and committing credit card fraud.

The personal characteristics of terrorists are non-static. Terrorists, especially Al-Qaeda related, are sensitive to investigative and regulatory scrutiny. Their characteristics

continuously evolve in an effort to avoid detection. They have taken on characteristics of individuals more identifiable with western societies. When assessing characteristics, you must consider the evolution of operational dynamics and consider factors to include operatives, targets, financing, and communications. Operatives have become more identifiable with their country of operation. Targets have become increasingly soft. The Madrid and London train bombings are somber references. Financing has increasingly centered on criminal activity. This places the operatives at higher risk of detection.

Indicators to look for can be varied. They should take on greater or lesser significance dependent on risk and vulnerability factors. Numerous sources, including FinCEN, the Financial Action Task Force and the Federal Financial Institutions Examination Council Examination Manual, have published reports and typologies listing money laundering and terrorist financing indicators.

## Conclusion

Best practices for detection and prevention of credit card information theft and fraud by terrorists include:

- **Identifying risk**

Credit card information is extremely vulnerable to exploitation and fraud. Identifying risk factors and taking steps to reduce risk will diminish vulnerabilities.

- **Understanding terrorists adaptability**

Terrorists are non-static and adapt to exploit systemic vulnerabilities and seize opportunities to steal credit card information and commit credit card fraud. To mitigate risk, businesses should implement and maintain robust information security programs. This should be considered essential and emphasizes the importance of security technology.

- **Vigilance**

Businesses are vulnerable to terrorist exploitation. They must monitor their systems and safeguard information and funds. Businesses should take proactive steps to develop and implement mechanisms to identify emerging trends.

- **Training**

Programs should be developed and implemented to educate employees about the vulnerabilities to credit card information theft and fraud. In addition, they should be given an overview of terrorist financing and how credit card information theft and fraud facilitates terrorism.

Everyone having responsibilities that may include compliance, anti-money laundering, risk management, information security, fraud, investigations, and monitoring are on the front line of the economic or financial component of the war on terrorism. Each of these functions has the direct or indirect potential to deny terrorists the opportunity to raise, move, and access funds. Denying terrorists funding has a direct bearing toward enhancing our National Security. Everyone should be mindful of this fact in their area of responsibility and be more vigilant in executing their duties. You may never encounter a terrorist or terrorist supporter, however...you may.

As previously mentioned, terrorist financing is extremely difficult to identify and deal with. It is possible to detect terrorist financing but not highly probable. Therefore, methodologies must be developed and implemented to increase the probability of detection. Methodologies must also be developed, enhanced and implemented to safeguard financial and credit card information from theft and exploitation. Forming an understanding of the multiple dimensions of terrorist financing will facilitate development of methodologies to detect, deter, and prevent the funding of terrorism.

**Disclaimer**

The information provided herein is for informational purposes only. This paper is not meant as compliance advice. Prior to taking any steps that may affect your compliance status with industry or government mandates always seek advice from your compliance auditor and/or legal counsel.



[www.shift4.com](http://www.shift4.com)

1491 Center Crossing Road  
Las Vegas, NV 89144-7047  
**Office:** (702) 597-2480

1453 South Dixie Dr., Ste 250  
St. George, UT 84770-5854  
**Office:** (435) 628-5454

**Support:** (866) 980-4446  
**Sales:** (800) 265-5795  
**Fax:** (702) 597-2499