DON'T BE A VICTIM

quarterly industry report

2012 Q2

scambook

Thank you for viewing the Scambook Second Quarter 2012 Report.

Scambook is an online complaint resolution platform. Anyone can fall victim to fraud, regardless of age, gender, race, nationality, education level, economic status or disability. At Scambook, our goal is to find justice for fraud victims and prevent future exploitation by building communities and educating the public with resources such as this Report.

We begin this Report with an introduction to Scambook, including a statistical overview concerning the prevalence of fraud in the United States. In this section, we will provide exclusive data about the Top 10 Most Affected States in the U.S. for Q2 2012 and compare this data to figures gathered in Q1.

Then, we will move on to Fraud in Focus. This section provides an in-depth industry analysis of the four most aggressive, widespread fraud schemes for Q2 2012:

- **Fake Job Offers**
- **Smishing/Text Message Fraud**
- **Phishing/Email Fraud**
- **Unauthorized Credit Card Charges**

For each Fraud in Focus, we will summarize the fraud scheme, provide background context, disseminate data gathered from our users and describe a Case Study that exemplifies the fraud scheme.

Each section will also include expert Warning Signs and Safety Tips addressing each specific fraud scheme. In addition to our Fraud in Focus analysis, this Report contains general Consumer Safety Tips, Testimonies from actual Scambook members and External Resources

We encourage you to download this Report and share it with your community. We hope this Report will serve as an educational guide for consumers, empowering them with the information they need to avoid falling victim to fraud. We also believe that this information can be a helpful tool for businesses seeking to reassure their customers.

Sincerely,

The Scambook Team

ABOUT SCAMBOOK

Who We Are and What We Do

Scambook is the internet's leading complaint resolution platform for consumers and businesses. Today, online communication and mobile technology are more widespread than ever. Unfortunately, criminals have adapted and learned to exploit this.

We've observed a distinct rise in fraud, identity theft, false advertising, phishing/smishing and unauthorized credit card charges related to new technology.

We created Scambook as a place on the web where people can fight back and arm themselves with the information they need to stay ahead of the latest emerging fraud schemes. In Q2 2012 alone, Scambook helped resolve $750,000 in complaints.

This Report is based on a sample of over 100,000 complaint reports submitted by our members.

"Yesterday i filed a Dispute Resolution on PayPal and they have already credited my credit card. This was the 1st time I'd been Scammed ... I will be using Scambook in the future to Search for any other company I want to deal with online." -- Actual Scambook Member

WHAT PEOPLE ARE SAYING ABOUT US

USER TESTIMONIALS

"Tried to buy NFL tickets on craigslist a woman named Alicia Martins claimed to be a British Airway employee who won ticktes. Did research and found an almost identical scam. Thanks Scambook.[sic]"

"Received a letter that I was a winner of a lotto and sweepstakes for the amount of $250,000.00. Fortunally, I when to the internet and surf this company out, thanks to Scambook, this Company was listed as a scam/false advertisment. [sic]"

"thanks to scambook I didn't lose a dime I started to order the ezeyes keyboard and seen the scambook report thanks scambook. [sic]"

"I recieved a text message from 13172209276 claiming that I won $1,000.00 Thanks to scambook, I will NOT fall for this scam... Thank you! [sic]"

"They sent me a letter in the mail stating if I sent $20.00 by check they would give me a check in return for $2,342,000.00 dollars. I of course didnt send any money because if something seems this good to be true I research it first! Thanks ScamBook! [sic]"

"when I got up the morning I google searched her name to see if I could find an address for her, and this scambook came up. I know I would have been out only ten bucks, but still she is a fraud. Thanks Scambook[sic]"

STATISTICAL OVERVIEW

Fraud Across the United States

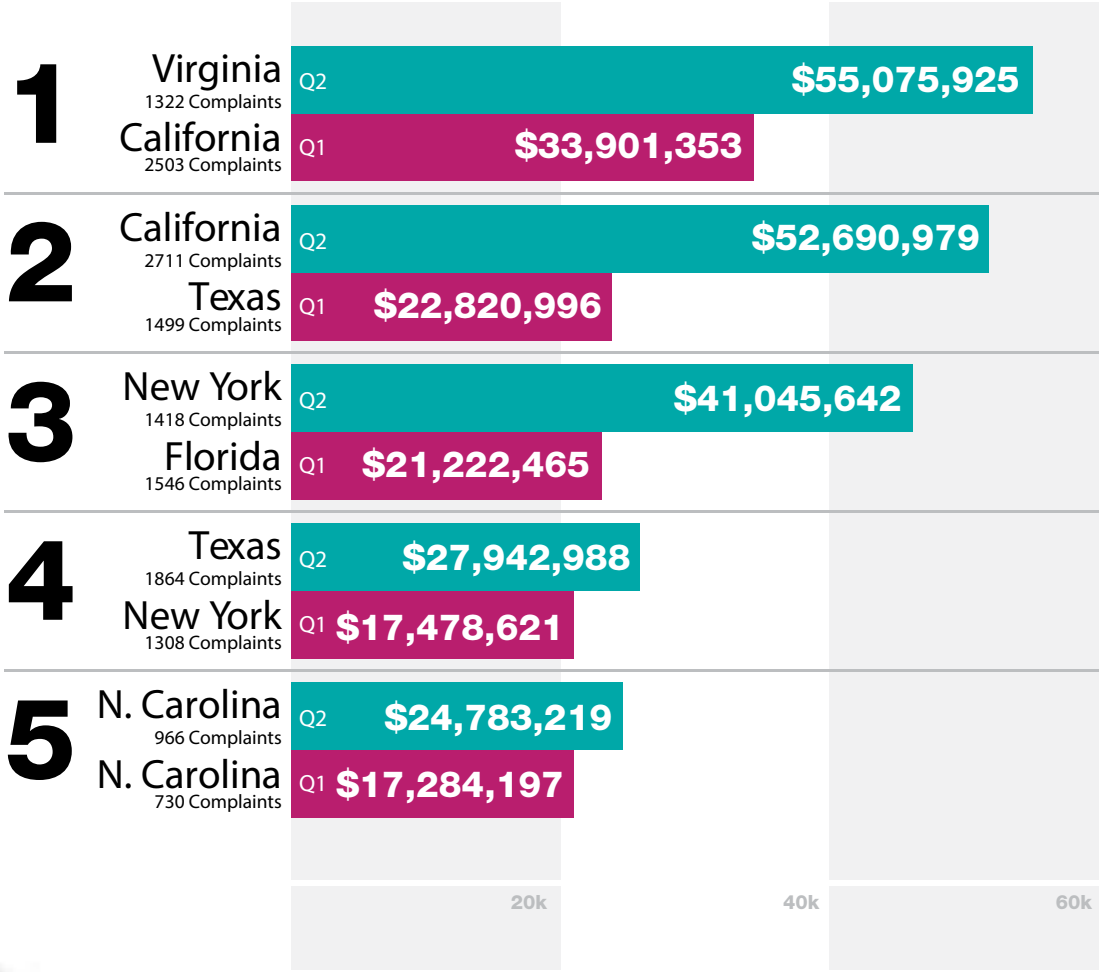
Overall, fraud claims an estimated $48 billion in damages every year. The Federal Trade Commission reports that 30 million Americans over age 18 were victimized by consumer fraud during a one-year period. 27.3 million people are estimated to be affected by identity theft.[i]

Here's What We See on Scambook

- **Overall, Scambook members report an average of $10,948.17 in damages per complaint.**
- **Average reported damages rose 65% in the Second Quarter 2012 – up to $16,828.25 in Q2 from $10,169.88 in Q1.**

TOP 5 STATES RANKED BY REPORTED MONETARY DAMAGES, 2012 Q1/Q2

In Q2, Virginia broke into the Top 5 and surged ahead of California for highest total reported damages.



"Thank god I found this site! was seriously thinking about buying these tickets, thank god she/he uses the same old British airways story!. and 150.00 price Thanks Scambook!"
-- Actual Scambook Member

COMPLAINT RESOLUTION PLATFORM

Report. Notify. Resolve.

At Scambook, we're consumers, too. We understand how it feels to be wronged or deceived with nowhere to turn for justice. That's why we pioneered the Complaint Resolution Platform.

Scambook provides a comprehensive, professional online support network for people who have been affected by poor business practices or fraud. Our Complaint Resolution Platform gives users a forum to air their grievances when other resources are unable or refuse to help.

Here's How Scambook Helps

- **Scambook users can submit complaints about companies, individuals, products or phone numbers.**
- **We organize complaints into groups and then connect users with one another to foster a community of group justice.**
- **Through the Scambook Dashboard, users can monitor the status of their report.**
- **We notify users of any changes or updates to their report.**
- **Then, utilizing Scambook Business Resolve, we reach out to the companies that our users report. We offer these companies an opportunity to directly resolve the issue with the consumer on Scambook.**

Our long-term goal at Scambook is to revolutionize customer service and reduce or eliminate conflicts between consumers and businesses.

We're confident that our Complaint Resolution Platform can adapt to meet the needs of a wide variety of industries. We hope that businesses will rely on Scambook to maximize efficiency, fulfill their customer service needs and improve their customer reputation.

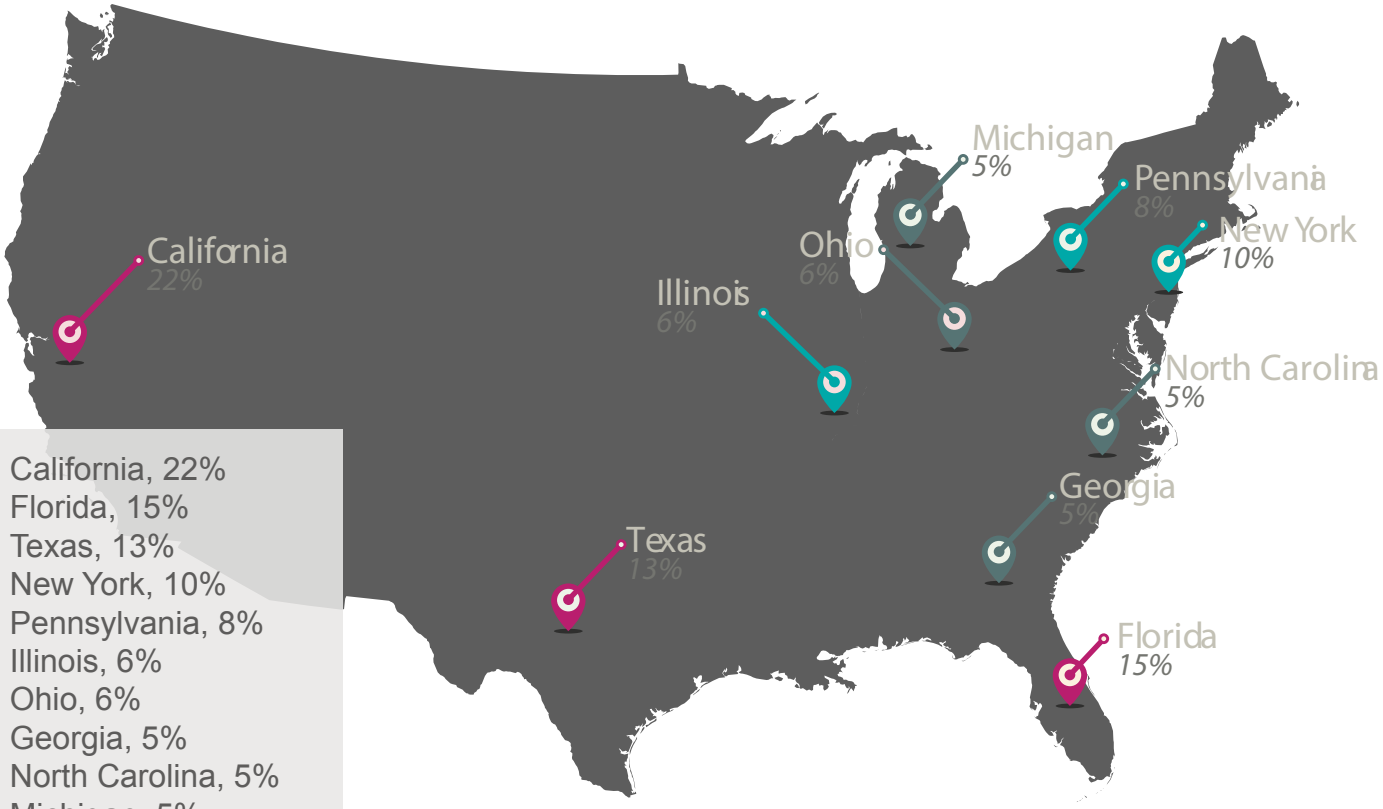
"I was just about to call [the fraudulent company], until I read these comments. Thanks scambook!" -- Actual Scambook Member

SCAMBOOK MEMBERS

Here are some of our user-reported demographics:

Top 10 States by Scambook Membership:

California, Florida, Texas and New York lead the U.S. in Scambook Membership.



California, 22%
Florida, 15%
Texas, 13%
New York, 10%
Pennsylvania, 8%
Illinois, 6%
Ohio, 6%
Georgia, 5%
North Carolina, 5%
Michigan, 5%

Membership by Gender:

Based on the profile information provided by our members, 43% of Scambook users are male and 56% are female.

"I just saw another person on Scambook complaining about this so it is a fraudulent trap to get people to sign on." -- Actual Scambook Member

FRAUD IN FOCUS

At Scambook, our complaint reports provide an exclusive look at the types of fraud affecting consumers today.

We view each complaint as a direct, primary source document on the schemes and deceptions that are used to exploit our members. By grouping individual complaint reports and placing them within the wider context of our international database, Scambook can determine what's trending in the world of fraud.

Scambook's insight is new and unique because it comes from the best possible source on fraud: you, our members.

The following pages will summarize the four most aggressive, widespread fraud schemes we identified in Q2 2012:

- **Fake Job Offers**
- **Smishing/Text Message Fraud**
- **Phishing/Email Fraud**
- **Unauthorized Credit Card Charges**

We've analyzed these trending schemes based on a thorough review of our members' reports. The follow pages will describe how the fraud works, provide background context, disseminate Scambook's complaint submission data for each type of fraud and document a Case Study that exemplifies the scheme.

We have also included case-specific Warning Signs and Safety Tips devised by our team of fraud experts.

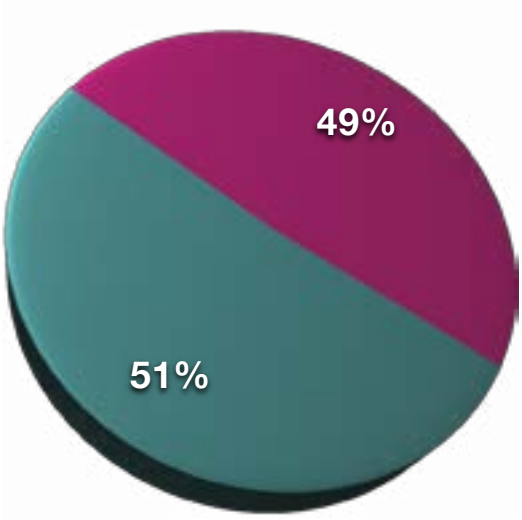
Information is the best defense against any type of fraud. We strongly encourage you to read this section carefully and share our security recommendations with your community.

FAKE JOB OFFERS

SUMMARY

- Criminals exploit job seekers with fake employment offers.
- Victims are usually unemployed, under-employed or looking to supplement a fixed income such as Social Security/Disability.
- Schemes are primarily conducted online through sites like Craigslist.
- These fraudulent job listings use keywords such as “work from home,” “secret shopper,” “career staffing,” and “no experience necessary.”
- Consequences include identity theft, unauthorized credit card charges and
- financial hardship caused by counterfeit money orders and wire transfers.

Percentage of Fake Job Offer Scams



In the second quarter of 2012, fake job offers Composed almost half of all false advertising complaints.

Fake Job Offer Scams

“After a gut feeling, I decided to write tabbulldogs.com SCAM into google and it sent me here. Luckily I sent no money. Thanks scambook.” -- Actual Scambook Member

Background:

Although the economy is recovering, the rate of job growth in the United States did not see a significant rise in the Second Quarter of 2012. Unemployment continues to hover around 8.2 percent, with approximately 5.4 million individuals on long-term unemployment for 27 weeks or more[ii].

This means that job seekers are still diligently searching for work. Many job seekers turn to the internet for help with job placement, searching on websites like Monster, Careerbuilder, LinkedIn, SimplyHired and Craigslist to find job listings. There are thousands of legitimate businesses and employers using these sites to hire new workers.

Unfortunately, criminals are taking advantage of eager online job seekers. They post fraudulent job listings to acquire credit card numbers and other personal information from innocent people. Criminals use this information to commit identity theft.

Based on reports submitted to Scambook, a majority of these victims are already struggling financially. Some victims are single parents or individuals on a limited fixed income, such as seniors and people with disabilities.

Users respond to fake job listings that seem tailored to their situation, with ads promising they can "work from home" or get paid for daily activities they already do, like shopping. Other fake job offers, using the keywords "career staffing," describe vague positions that require little to no prior experience.

In some instances, criminals will obtain an individual's contact information from an online resume. They cold call or email the victim, claiming to be a Human Resources representative, and thereby lull victims into a false sense of security.

Another type of job offer fraud asks job seekers to pay for a book or an "info kit" to start working from home. Users who purchase these items never receive them.

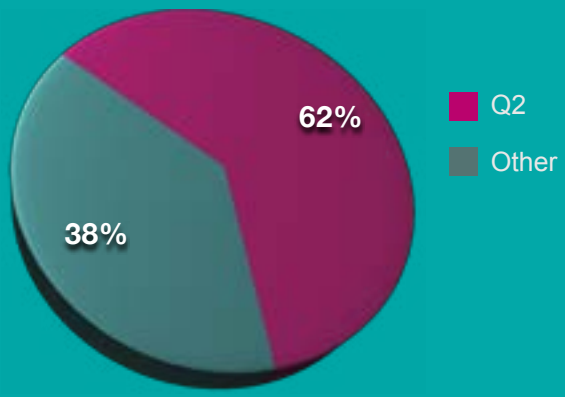
The following pages will identify the Top Trending fake job schemes of Q2 2012.

A fake job ad might look something like this.

CASE STUDY
1st PREMIER STAFFING

AT A GLANCE

1st Premier Staffing is a fraudulent company that posts fake job listings on Craigslist. They claim to hire receptionists, warehouse supervisors, customer service, security and other various positions. When job seekers respond to the fake ads, 1st Premier Staffing asks for their Social Security Number or credit card number.



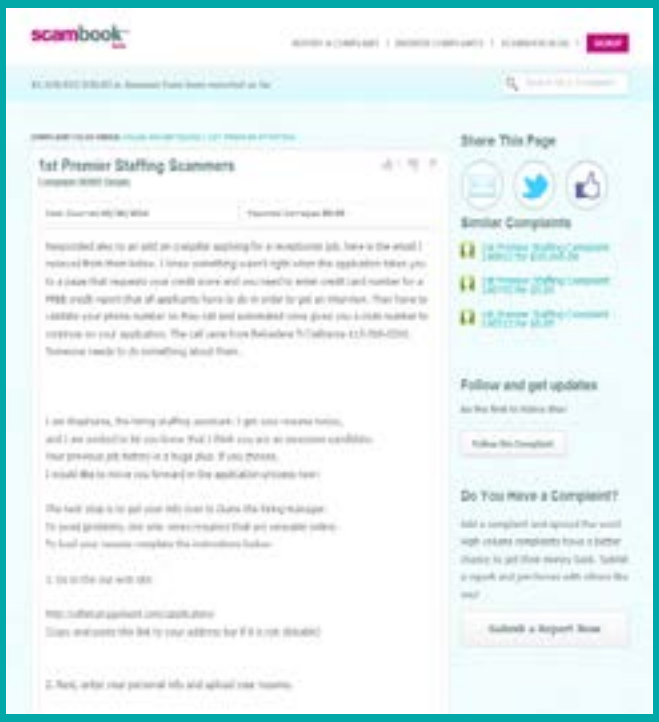
In Q2 of 2012, 1st Premier Staffing Complaints represented 62%.

Quick Stats

$3,527,644
Total Reported Damage

HOW IT WORKS

1st Premier Staffing claims to hire receptionists, warehouse supervisors, customer service, security and other various positions. Scambook members who respond to these ads receive the same automated reply (although the name of the staffing assistant changes from report to report).



Hello _____,

I am Wilfred, the hiring staffing assistant. I got your resume today, and I am excited to let you know that I think you are an awesome candidate. Your previous job history is a huge plus. If you choose, I would like to move you forward in the application process now!

Hello Melody,

I am Marlene, the hiring staffing assistant. I got your resume today, and I am excited to let you know that I think you are an awesome candidate. Your previous job history is a huge plus. If you choose, I would like to move you forward in the application process now!

The next step is to get your info over to Diane the hiring manager. To avoid problems, she only views resumes that are viewable online. To load your resume complete the instructions below:

1. Go to the our web site:

http://boygrmgm.com/application/
(Copy and paste this link to your address bar if it is not clickable)

2. Next, enter your personal info and upload your resume.

IMPORTANT! Each applicant is required to have a personal application code in order to fill the application.

Your code is: Eb0gFEDc8

Let me know when you finish the instructions.
If you don't contact me by tomorrow I'll assume that you are not interested in the job, and I'll go on to the next candidate.

Melody, you're a decent candidate for the job, but I will move on to the next candidate if I have to.

Marlene
1st Premier Staffing

HOW IT WORKS

CONTINUED

In some cases, Scambook members report that they simply responded to the ad with a question – they didn't send their resume or mention their job history. But the "hiring staffing assistant" always praises their experience or job history in the opening paragraph.

After this introduction, users are directed to an online application, asked to enter a code and then prompted to do one of two things:

- **Submit their Social Security number for a background or credit check.** Although many employers do screen potential recruits, it's a huge red flag if they require sensitive personal information before they interview you.
- **Enter their credit card number to receive a "free" trial of something called Privacy Guard.** This free trial expires almost immediately and users are charged for shipping, processing or other fees. However, even if this service didn't require a user's credit card info, it's very suspicious that a company would require you to subscribe to something in their first email.

At the end of the fake letter, the staffing assistant tells individuals that they are "a decent candidate for the job, but I will move on to the next candidate if I have to."

This is another important warning sign. Criminals who commit fraud often pressure you to act right away or make threats if you respond too slowly. The job market can be very competitive, but legitimate employers don't need to pressure you like this.

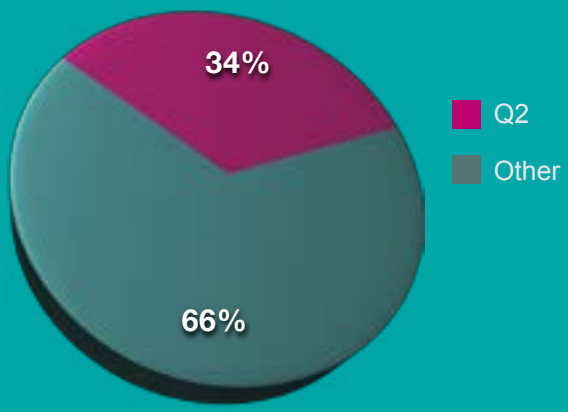
SIMILAR SCHEMES

Wellman Careers & Partners
78 Complaints / $32,437 Report Damages

CASE STUDY
SECRET SHOPPER

AT A GLANCE

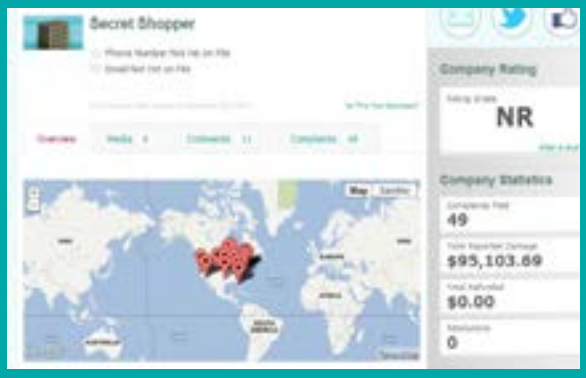
Secret Shopper recruits job seekers to go on mystery shopping “missions” at retail stores such as Walmart, Target or Best Buy. They send the victim a huge check or money order to cover their expenses. The victim is instructed to cash this check or money order, keep what they’re owed and wire the rest of the money back to the sender. Unfortunately, these checks or money orders are counterfeit, leaving the victim in a tight spot.



In Q2 of 2012, Secret Shopper Complaints represented 34%.

Quick Stats

$95,103
Total Reported Damage



HOW IT WORKS

For people with a low or fixed income and limited transportation, such as students, the elderly and disabled people, these job listings sound like a perfect opportunity. They often advertise "no experience necessary." According to Scambook members, the ads on Craigslist and other websites ask job seekers to:

- **Shop at retail stores like Walmart, Target, Best Buy or grocery stores. Often, these are stores that the job seeker already patronizes on a regular basis.**
- **Interact with store employees and management, make notes about the store layout and record other observations. Shoppers are occasionally given lengthy surveys and asked to rate their experience on various criteria.**
- **Keep any items you purchase on your secret shopping trip – anything from household goods to high-end electronics – and receive additional compensation for your time.**

It's important to note that there are legitimate agencies that hire secret shoppers, also known as mystery shoppers or mystery consumers. Marketing firms and consumer watchdog groups value the input of everyday people. In some cases, retailers will also hire mystery shoppers to test their own infrastructure.

QUICK TIP

Watch out for secret shopping jobs that ask you to evaluate a money transfer service like Western Union or Money Gram. These are always fraudulent.

HOW IT WORKS

CONTINUED

Unfortunately, it can be very difficult to distinguish between a real secret shopper job and a fraud scheme.

Job seekers who apply to fake mystery shopping schemes, such as the hoaxes perpetrated by organizations like Secret Shopper, find that they are always approved after they respond to the ad. Without speaking to anyone over the phone or exchanging follow-up emails, victims are instructed to start immediately.

Within a few days, the victim receives a check or money order from Secret Shopper. These checks and money orders are usually in the amount of $1000 or more. This is a much greater sum than the $200 or $300 compensation promised to the victim.

The victim is instructed to cash the check, withhold the amount they are owed and send back the rest of the money via Western Union. In many cases, the recipient name and address may be different from the original sender. This third party recipient is in often another state or even overseas.

Sadly, these checks and money orders are ultimately determined to be counterfeit. Financial institutions are required to make the funds from deposited checks or money orders available within days, but discovering counterfeits can take weeks. Once this happens, the victim is held liable for repaying the bank. At Scambook, we have received reports of victims who have lost their life savings in these schemes.

We advise consumers and job seekers to use extreme caution when applying to secret shopper positions. If you respond to an ad for a secret/ mystery shopper position, we recommend that you follow these safety guidelines:

- **Don't give out any personal information (such as mailing address, bank account or credit card number, PayPal password or Social Security number) via email**
- **If someone wants to hire you to be a secret shopper, ask to speak with them on the phone, meet in person or at least exchange additional email messages**
- **Research the organization on Scambook and the web.**
- **Ask questions. A legitimate organization will be happy to give you more information.**
- **If everything seems to check out and you do go on a secret shopping trip, don't buy items you can't afford on your own. Sometimes, you can't tell if you've been conned until your**

HOW IT WORKS

CONTINUED

first paycheck arrives. If this happens, you don't want to be stuck with payments for a high-end item.

- **Remember that legitimate businesses won't charge you any fees to begin working. They won't mail you a check or money order for the wrong amount and then ask for the extra money to be wired back. These are warning signs of fraud.**

The FTC also advises consumers to avoid mystery shopping jobs that guarantee the position or instantly approve your application, require you to pay for "certification," or require you to buy materials such as company directories[iii].

IIf you suspect you've been defrauded, take print copies of the original ad, emails from the criminal and all suspicious checks or money orders to your local law enforcement. We also suggest that you report the incident on Scambook.

SIMILAR SCHEMES

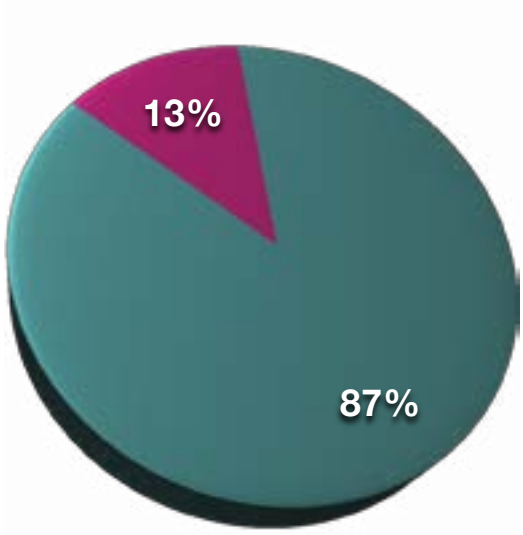
Mystery Shopper
$159,473 Reported Damages

SMISHING

SUMMARY

- The term “Smishing” is derived from “SMS” (text messages) and “phishing.”
- Spam text messages offering free gift cards and other prizes, which direct consumers to fraudulent websites asking for personal or financial information.
- Smishing text messages often originate from overseas.
- For many consumers, the cost of these spam text messages quickly adds up, leading to an increased wireless bill that strains their budget.
- Consumers are advised not to reply. Replying to a smishing message may result in unwanted charges and fees.

Percentage of Smishing Scams in Relation to Other Types of Scams



In the second quarter of 2012, smishing text messages composed 13% of complaint reports.

Smishing Scams

“Thanks to scambook I was able to report to Sprint the details of this scam. Sprint, my cell phone provider, took care of these scammers and I’ve been reimbursed.” -- Actual Scambook Member

Background:

According a recent retrospective in The Guardian, SMS (short message service) text messaging was created by a special committee of European telecomm companies in the 1980s. Texting has grown tremendously ever since. It's estimated that two-thirds of the world's population (approximately 4 billion people)[iv] send and receive text messages on their mobile phones.

As with any new technology, con artists soon learned to exploit SMS text messaging to steal from honest, hard-working mobile phone users.

Prior to the introduction of mobile internet, the earliest smishing messages warned recipients that had been subscribed to a paid service. They claimed that the recipient would be charged $2 a day until they cancelled by visiting a certain website. These websites inevitably infected the recipient's computer with a virus or other malware that would steal sensitive personal information.

Today, smishing messages are much more complex and varied. The danger is also increased because of the widespread use of smart phones. Mobile devices like the iPhone and Android phones can hold more private data than ever before, everything from email to bank account information. Hackers no longer need access to a consumer's computer to obtain their passwords or other sensitive data.

Spammers can also exploit mobile phone technology to automatically register consumers for unwanted fees and monthly charges. Replying to a smishing message, even with the word "UNSUBSCRIBE," can lead to an unpleasant surprise on the consumer's next phone bill.

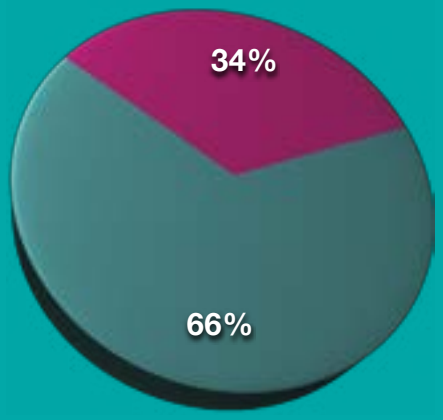
Today's smishing messages also include links to external sites. One very popular scheme says that consumers have won gift cards, sweepstakes money or other prizes. They are instructed to visit a certain website to redeem their prize, however, this website prompts them to complete a series of bogus surveys and give out their personal information. This can lead to unauthorized credit card charges and other identity theft.

The following pages will outline one of our Top Trending smishing frauds for Q2 2012, the Walmart Gift Card scheme.

CASE STUDY
WALMART GIFT CARD

AT A GLANCE

Victims of this fraud scheme receive a text message saying they have won a $1000 Walmart gift card. The message directs the victim to a website that mimics the real Walmart site, where they are asked to give their personal information or credit card number to complete a survey.



In Q2, Walmart Gift Card Complaints made up 34% of all Smishing Complaints.

Quick Stats

$3,215,940
Total Reported Damage

1,223
Complaints

HOW IT WORKS

The Walmart Gift Card scheme remains a top offender on Scambook. We received our first complaint about this fraud in November, 2011. Unfortunately, consumers continue to be targeted and the trend hasn't slowed down. Although we've covered this fraud in the Scambook Q1 report, we feel its continued prominence requires additional analysis.

Here's how the Walmart Giftcard Smishing Scheme typically works:

- **Users receive a text message saying they have won a $1000 Walmart Gift Card. The message includes a link to a website, occasionally accompanied by a promotional code.**
- **On this website, users are prompted to complete a series of surveys, purchase special offers and/or submit their personal information.**
- **Users never receive the gift card. Instead, they find themselves hit with mysterious monthly charges for subscription services. These charges can appear on their credit card bill, mobile phone bill or both.**
- **When users attempt to contact the companies and cancel these subscriptions, they find it very difficult (even impossible) to reach customer service and obtain refunds.**

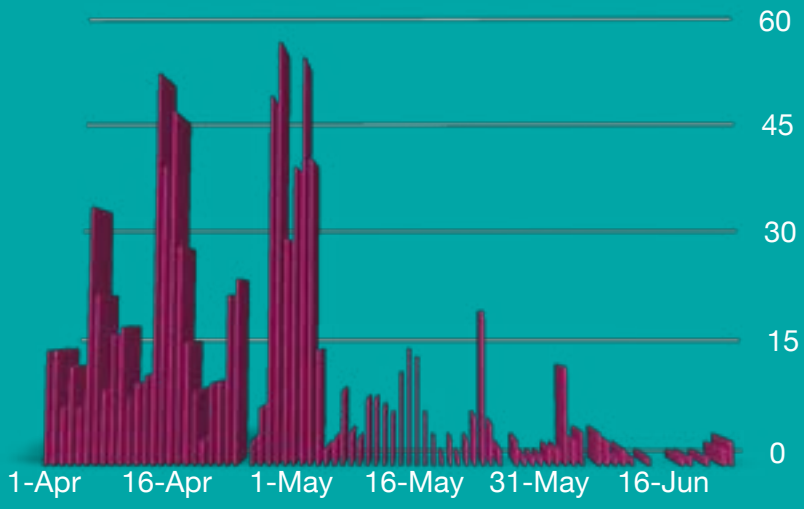
It's important to note that the gift card offer isn't affiliated with or endorsed by Walmart. Similar schemes use Best Buy, Target and other retailers as bait for unsuspecting consumers.

While this incarnation utilizes SMS text messages, we have found that this bonus gift card offer also appears in spam emails ("phishing") and on social media networks such as Twitter, Facebook, Pinterest and Instagram.

We received our first complaint about this fraud in November, 2011. Complaint submission peaked near the end of Q1, however Q2 saw a 62% increase in overall complaints – a total of 889 complaints, up from 335 in the previous quarter. This increase was concentrated near the beginning of Q2 and tapered off in June, but members continue to submit complaint reports about this smishing scheme.

HOW IT WORKS

Number of Complaints Submitted Per Day Against Walmart Gift Card Smishing, Q2 2012



Although complaint submission peaked in May, this fraud scheme continued to affect consumers throughout Q2.

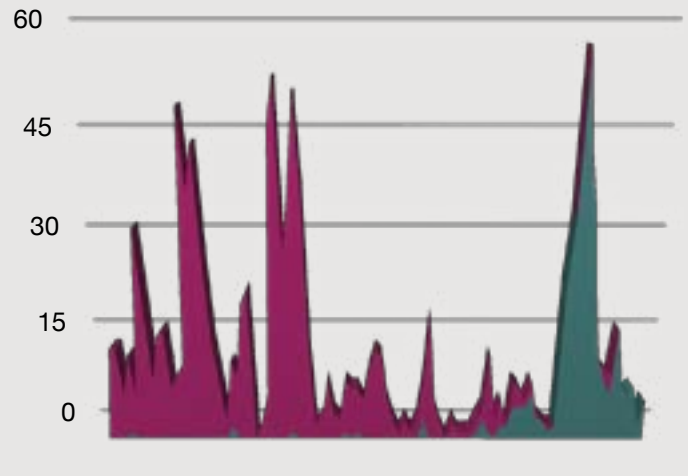
When you receive a smishing message for a $1000 Walmart gift card or a similar offer, DO NOT REPLY. The cybercriminals behind these text messages send them to thousands of random phone numbers. They don't necessarily know that your number is active. If you reply and tell them to "UNSUBSCRIBE," you will confirm that your number works. You may receive even more smishing messages or unwanted charges.

Don't click the link provided in the text. It may install malware or a virus on your computer.

Remember that legitimate companies will never ask for your private information in a text message. Additionally, if you've actually won a contest, a legitimate business will NOT ask you

Q2 vs Q1

Complaint submission rate for Walmart Gift Card fraud, Q2 vs Q1.



Data Source: Scambook.com

HOW IT WORKS

CONTINUED

to give your credit card information, purchase a subscription or otherwise give away your personal information to claim the prize.

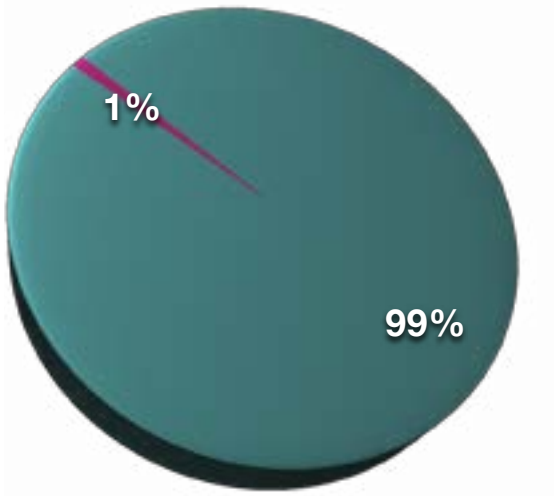
We advise consumers to ignore text messages from numbers they don't recognize and check their phone bill very carefully each month for unexpected charges. If you have been affected by mobile phone fraud, contact your service provider right away.

PHISHING

SUMMARY

- **The term "phishing" refers to spam emails that "fish" for a consumer's personal information, such as their credit card number, or online passwords.**
- **Phishing emails may take a variety of forms.**
- **Frequently, phishing emails imitate real companies like eBay and PayPal. They often include company logos and mimic the layout of a real customer service email.**
- **Phishing emails may also include malicious attachments or direct users to external websites that infect their computers with viruses and malware.**

Percentage of Phishing Scams



In the second quarter of 2012, phishing Complaints composed less than 1% of the total reports submitted. However, our research suggests that phishing plays a major role in many other types of fraud.

Phishing Scams

"He needed my paypal information, and needed me to forward a payment to his pick up agent, luckily caught before we sent anything. Thanks scambook!" -- Actual Scambook Member

Background:

The first known use of the word “phishing” was recorded in 1997[v]. However, experts estimate that the techniques used by phishing emails originated in the late 1980s. Early phishing emails targeted AOL users and stole their passwords, but hackers quickly realized they could use phishing to obtain credit card information.

Some phishing emails “bait” victims with special offers or prizes. Then, as with smishing fraud, they direct victims to download an attachment or visit an external website. Attachments usually carry viruses or malware that will steal the victim’s passwords and other information.

The website may also infect the victim’s computer. However, it frequently obtains the victim’s information because the victim volunteers it. These websites can be very clever spoofs of real sites like eBay, PayPal, Bank of America, Amazon or other online businesses. They may use the company’s real logo and mimic the layout of the legitimate site. Victims are therefore duped into logging in with their real username and password.

Other websites may resemble customer survey pages or special offers. DO NOT GIVE THEM YOUR INFORMATION. Cybercriminals will use your information to continue spamming you. They may also commit identity theft and begin charging your credit card.

QUICK TIP

If you realize you’ve given your login information to a bogus site, go to the real site, change your password IMMEDIATELY and email tech support to alert them that your account may be compromised.

“I received the same letter as described by others. I figured this was a scam and was glad to see it on Scambook. Thanks everyone for posting your info.” -- Actual Scambook Member

CASE STUDY
PayPai

AT A GLANCE

PayPai (with an “I”) mimics the name and style of a PayPal (with an “L”) customer service email. It directs victims to download an attachment or visit a fake website that steals the victim’s personal information. The PayPai email may also attempt to install viruses or other malware on the victim’s computer.

Quick Tip

If you receive a suspicious email, check the address of the sender. A phishing email will usually come from an equally suspicious domain, i.e. john@scammer.co.uk

HOW IT WORKS

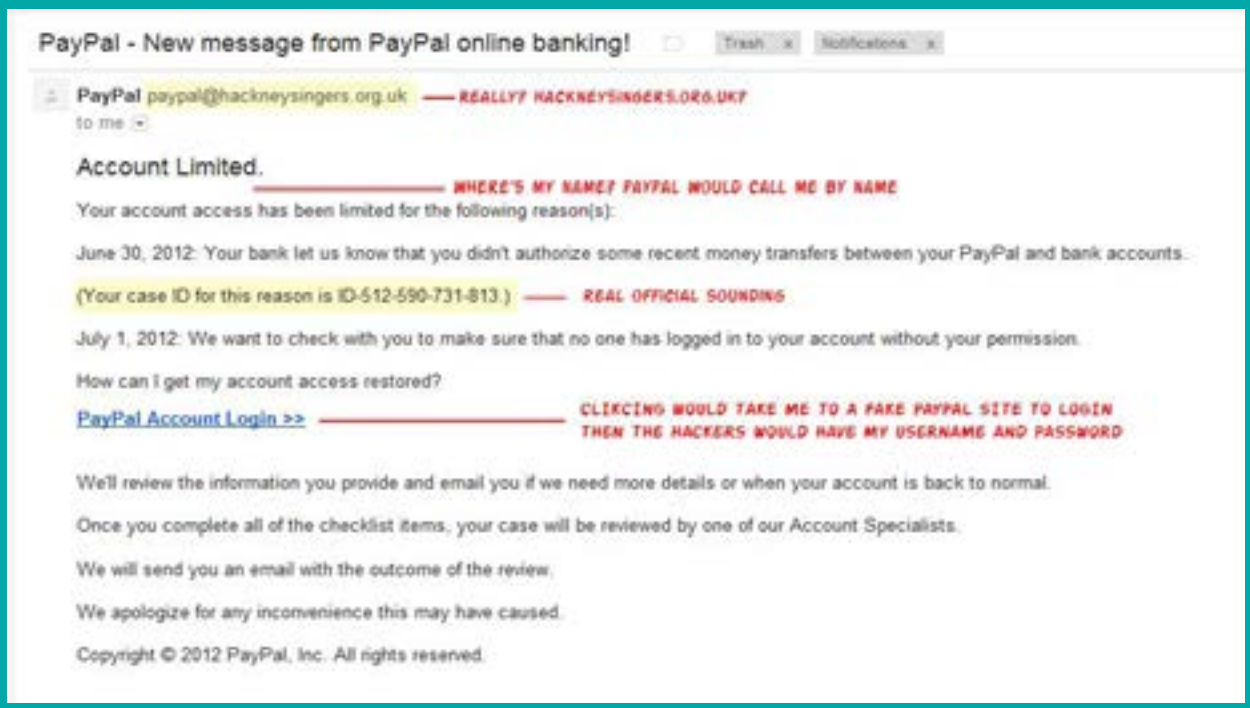
PayPai is a phishing scheme that relies on a linguistic device called a homograph. A homograph is a letter, number or symbol that looks identical to another, different character.

In this case, cybercriminals exploit the fact that a capital letter “i” can be almost indistinguishable from a lower-case letter “L” in certain san serif (tailless) fonts such as Arial. San serif fonts also happen to be the default font used in popular email clients like Gmail and browsers like Firefox.

The PayPai phishing email states that a victim’s account is “limited,” and it uses language that mimics an official email.

“Your bank let us know that you didn’t authorize some recent money transfers between your PayPal and bank accounts ... We want to make sure that no one has logged into your account without your permission.”

As with many other phishing schemes, PayPai is accompanied by a link to a fake website that prompts users to give their credit card information or the username and password for their real PayPal account.



HOW IT WORKS

CONTINUED

To avoid falling victim to phishing fraud like PayPai, we advise that consumers pay attention to the following details:

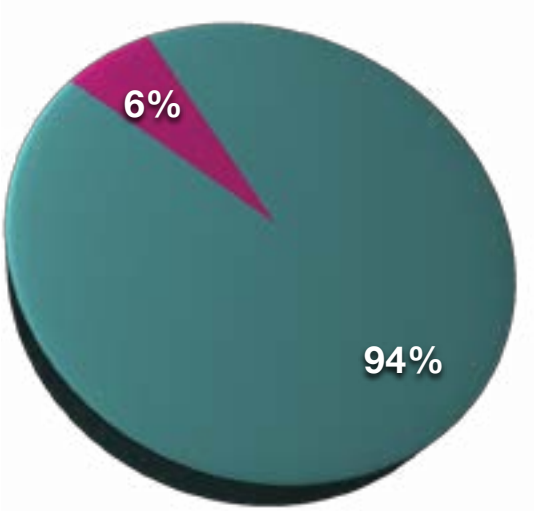
- **Look at the sender's email address. A real message from PayPal would come from an email address like support@paypal.com, but the PayPai email originated from an address at hackneysingers.org.uk.**
- **Examine the URL that loads in your browser. Do you see "https" in front of the website's address? The "s" at the end means that the website is more secure. For an online store, online banking service or other official websites that require your personal data, the "s" should be there. Be careful if it's just "http".**
- **Another red flag can be the website address itself. Is it simple, like www.eBay.com, or are there additional words, symbols and numbers? Phishing websites often include extra phrases and characters that don't make any sense. Watch out for web addresses such as "page.@ebay.com" or "signin-@ebay.com@21.3442.1". Foreign addresses can also tip you off. If you live in the United States, you shouldn't be getting emails from eBay's Hong Kong division.**
- **NEVER CLICK ON LINKS IN A SUSPICIOUS EMAIL. Remember that legitimate sites like eBay and PayPal will never ask for your username, password or credit card number in an unsolicited email. When in doubt, delete the suspicious email and open a brand new browser window. Go to https://www.paypal.com directly and then log in. If you do have an important message from PayPal, it will be displayed on your account page.**
- **When possible, notify the real company that a con artist is impersonating them and using their image. Sites like eBay and PayPal have special customer support division to address hackers who use their brand's likeness. They will appreciate your help and provide you with specific safety tips for their service.**

UNAUTHORIZED CREDIT CARD CHARGES

SUMMARY

- **An umbrella category that encompasses many types of consumer fraud and identity theft.**
- **Victims find themselves charged for products or services they didn't order.**
- **Charges may be part of a monthly subscription.**
- **Occasionally, victims are able to reverse the charges by calling the company associated with the charge.**
- **However, many Scambook members report that they have had to cancel their credit card account.**

Percentage of Unauthorized Credit Card Charges in Relation to Other Scams



In the second quarter of 2012, unauthorized credit card charges comprosed 6% of total complaint reports.

Unauthorized Credit Card Charges

"They caraged $84.00 To my credit card. They have as of this date refunded my money. Thanks to you for letting me put this on scambook." -- Actual Scambook Member

Background:

Unauthorized credit card charges are at the root of the majority of Scambook complaints. This type of financial fraud affects 10% of adults each year in the US[vi]. Unauthorized credit card charges are defined as unwanted, unexpected financial transactions on the cardholder's account that occur without the cardholder's consent.

This can occur for a variety of reasons. We find that websites with "free" offers or prizes are a prominent offender, registering users for paid monthly subscriptions without their explicit consent. The "free" offer expires within a few days and, unless users call customer service to cancel, they are charged a monthly fee.

We have received hundreds of reports about misleading offers for "free" credit reports, diet pills and more.

To avoid this type of fraud, we recommend that consumers:

- **Always read the fine print. Do not give your credit card number to any individual or website until you have read the entire terms of service agreement and privacy policy. If you don't understand what you're signing up for, don't submit your information. You can always research the company or product on Scambook and sign up at a future date.**
- **Check your bank account online every day and ALWAYS read your credit card statement. The sooner you notice an unexpected, unauthorized charge, the sooner you can call your financial institution to dispute it.**

QUICK TIP

If a special "free" offer is time-sensitive or you're being pressured by a sales representative to commit right away, it's a big red flag.

"… did some research and confirmed my suspicions. Thank you Scambook for the opportunity to let us know the pitfalls!" -- Actual Scambook Member

CASE STUDY
PREMIER MEMBERSHIP CLUB

AT A GLANCE

Members who report this complaint are charged $99.49 by a company called Premier Membership Clubs. Victims are confused by this unauthorized credit card charge because they have never ordered anything from Premier Membership Clubs. Scambook investigation has revealed that this company is affiliated with a variety of other websites, including payday loan sites, which victims may have done business with in the past.

Quick Stats

$783,509
Total Reported Damage

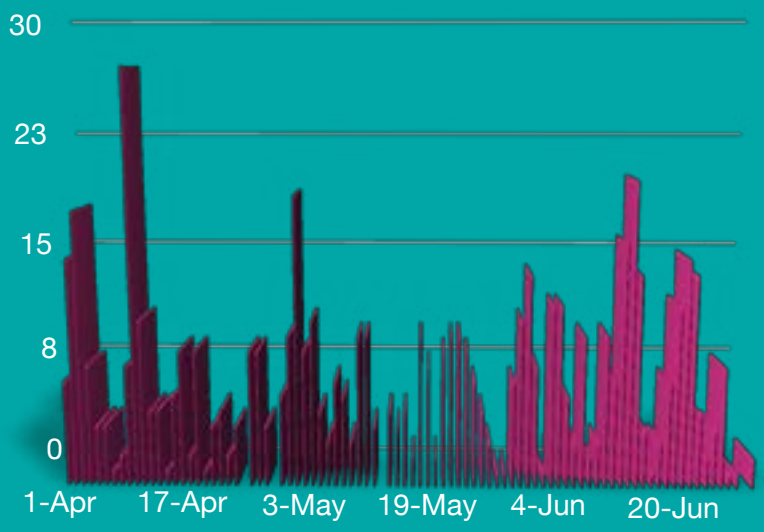
HOW IT WORKS

We began receiving reports against this company in August, 2011. Since then, complaints have followed an ebb-and-flow pattern, peaking on January 5 at 42 submitted complaints.

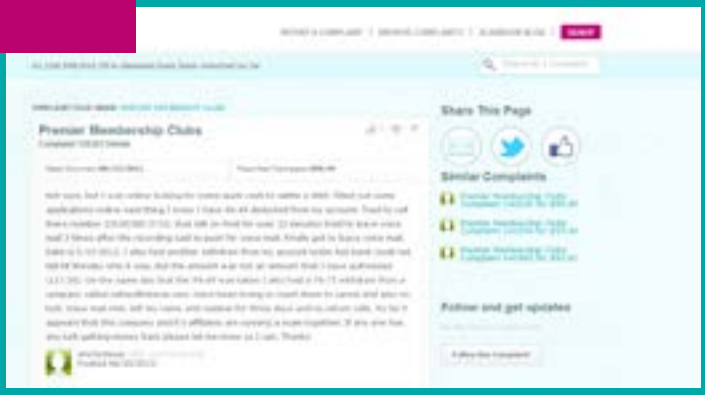
Complaints about Premier Membership Clubs fell 39% from Q1 to Q2.

Despite this decrease, Scambook members continue to submit complaints about this company at a relatively constant flow.

Number of Complaints Submitted Per Day Against Premier Membership Clubs, Q2 2012

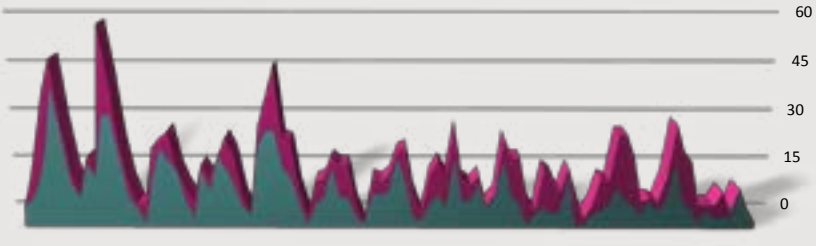


Submission rate for complaints against Premier Membership Clubs was steady in Q2.



Q2 vs Q1

Complaint submission rate for Premier Membership Clubs, Q2 vs Q1.



Data Source: Scambook.com

HOW IT WORKS

CONTINUED

Premier Membership Clubs (PMC) is a third-party customer service company that also operates as YourSupportDepartment.com and YourCustomerServiceOnline.com.

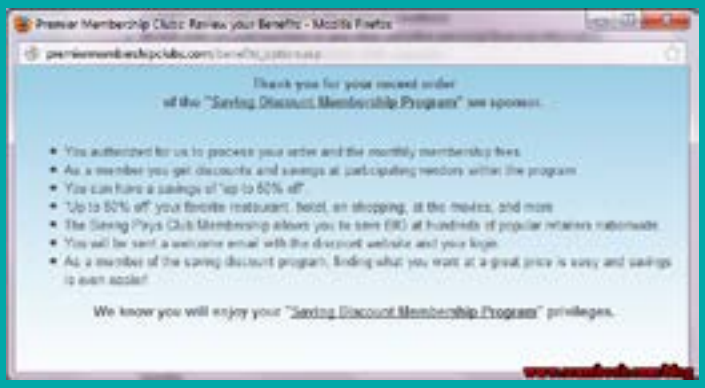
They are also associated with the discount club SavingPaysYouNow.com and the payday loan site CashLoan.com.

PMC charges a $99.49 fee to consumers who apply for payday loans and other online services. However, victims of this unauthorized credit card charge did not intend to sign up for PMC's membership. They are automatically enrolled when they acquire a payday loan or use another service from one of PMC's affiliate sites. This automatic enrollment is buried in the affiliate site's terms of service and it's very easy to miss.

Victims of this unauthorized charge report that they are usually struggling financially, and PMC's $99.49 charge is a burden they can't afford. Scambook has received reports about this company from single parents and people on limited fixed incomes. According to a recent press release from Pioneer Services, PMC has also taken advantage of military families by falsely representing Pioneer Services, a financial institution serving active duty military, veterans and their families[vii].

Although some Scambook members have reported that they have been refunded by PMC customer service, others say they have had to cancel their credit card to get the charges to stop.

We recommend that you avoid this unauthorized credit card charge by using extreme caution whenever giving your personal or financial information online. We also hope that you will share this information with your community and educate others about this unethical company.



CONSUMER SAFETY TIPS

- When making online purchases or submitting sensitive personal data, be very careful. ALWAYS read a website's terms of service and privacy policy. Don't give out your information without understanding the full user agreement.
- Be wary of suspicious emails with urgent requests for personal financial information, as well as any unsolicited text messages and phone calls that require sensitive personal information.
- Create online passwords that are difficult to guess. Secure passwords use a mix of uppercase and lowercase letters, numbers and symbols, i.e. Ca4tL0v*3Rr#7892. Never use information that could be easy to guess, like your birthday or the name of your street. We recommend that you create a different password for every site you use. For additional security, you should change your passwords every 3 months.
- NEVER give out your checking account number over the phone unless you know the company and understand why the information is necessary. Also, be on guard against rudeness and intimidation – if a salesperson is pressuring you to buy, without giving you time to research the product or company, it's a red flag.
- When purchasing infomercial products, pay close attention to the total cost. This includes shipping and handling for each item, not just the advertised "special" price.
- When making a donation, obtain as much information as possible about the charity – including the name, address, phone number and the name of a contact person if possible. Research the organization before you give them any personal or financial information.When you're traveling, ALWAYS review your hotel and vacation itinerary. Make sure you fill out your passport, sign it and fill out the emergency information.
- Check your bank account every day if possible and ALWAYS read your bills. The sooner you notice an unauthorized charge, the easier it will be to remedy. We suggest that you check your bank account and review your bills electronically as part of your regular online routine, i.e., login to your bank right after you check your email. If you need help keeping track of your finances online, try Mint.com

EXTERNAL LINKS

[i] Scambook.com, “Scambook 2012 Q1 Market Report.” http://www.scambook.com/press/scambook_market_report_q1_2012

[ii] Bureau of Labor Statistics, “Economic News Release: Employment Situation Summary.” http://www.bls.gov/news.release/empsit.nr0.htm/

[iii] Federal Trade Commission, “The Secrets of Mystery Shopping...Revealed.”

http://ftc.gov/bcp/edu/pubs/consumer/alerts/alt151.shtm

[iv] The Guardian, “Now 4 billion people know the joy of txt.”

http://www.guardian.co.uk/technology/2012/may/06/sms-text-messages-20th- birthday

[v] Mirriam-Webster Online, “phishing.” http://www.merriam- webster.com/dictionary/phishing

[vi] StatisticBrain.com, “Credit Card Fraud Statistics.”

http://www.statisticbrain.com/credit-card-fraud-statistics/

[vii] PioneerServices.com, “Pioneer Services warns military about Premier Membership Club scam.”

http://www.pioneerservices.com/newsroom/releases.cfm/Pioneer-Services- warns-about-scam-from-Premier-Membership-Club