Scambook

Quarterly Industry Report
2012 Q3

Executive Summary

Thank you for viewing the Scambook 2012 Third Quarter Industry Report.

Scambook is an online complaint resolution platform for consumers and businesses.

Anyone can fall victim to fraud and bad business, regardless of age, gender, race, nationality, education level, economic status or disability. At Scambook, our goal is to facilitate complaint resolution between consumers and businesses, help fraud victims find justice and prevent future exploitation by building communities and educating the public with resources such as the Scambook Third Quarter Industry Report.

This Report is based on a sample of more than 100,000 user-submitted complaints. Since its inception, Scambook has resolved over $3 million in reported damages between consumers and businesses. In the Third Quarter dating July 1, 2012 to September 30, 2012, our platform facilitated over $895,000 in resolutions.

We begin with an introduction to Scambook, including a review of Scambook's complaint resolution process, a statistical overview and a real Scambook Success Story. In this section, we will provide exclusive data about the Top 5 Most Affected States in the U.S. for Q3 2012 and compare this data to figures gathered in Q2.

Then, we will move on to Third Quarter Trends. This section will begin by emphasizing the impact of fraud nationwide, with a brief summary of Fraud Factors that increase consumer vulnerability. From there, we present the Top 3 Complaint Trends for Q3:

- **Free Best Buy $1000 Gift Card Texts**
- **HCG Ultra**
- **SurveyCruise.com**

For each of Top 3 Trends, we will summarize the complaint cases, provide unedited quotes to describe the trend in our users' own words, cite patterns based on Scambook's complaint submission data and analytics, and present expert Warning Signs and Safety Tips addressing each complaint trend. We conclude our report with General Consumer Safety Tips.

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 via Scambook's Complaint Resolution Platform.

We're passionate about what we do. As we review Q3 2012, we look back with an eye for innovation and positive change to carry forth our mission in Q4 and beyond.

Sincerely,

The Scambook Team

ABOUT SCAMBOOK

Who We Are and What We Do

Scambook lets consumers and businesses resolve complaint disputes in a secure, neutral space while educating the public about fraud.

We know it can be hard for consumers and businesses to reach an understanding when someone feels cheated or ripped off. Scambook was created as a safe platform where each party can resolve a dispute with greater speed and efficiency than traditional channels.

Our Complaint Resolution Platform is one of a kind and it's revolutionizing the way consumers and businesses interact. Consumers get their voices heard and get their money back. Businesses show the world that they're responsible and they care about their clients. Everyone wins.

Since its inception, Scambook has resolved over $2 million in reported consumer damages. In Q3 alone, our platform facilitated over $895,000 in resolutions between consumers and businesses.

We're also a community resource where users can come together, share their experiences and learn how to stay ahead of the latest trends in fraud and cybercrime. Cited by Forbes, Today.com, CBS.com, The Chicago Tribune and Investing Answers, Scambook is rapidly becoming a leading source for consumer news and fraud alerts.

Scambook believes that no one deserves to be victimized by fraud or bad business practices. We're passionate about what we do.

That's why we're blazing the trail for a brand new type of consumer service experience. Got a complaint? We'll get it resolved.

Over
$895,000
in resolutions

STATISTICAL OVERVEIW

Top 5 States Ranked by Reported Monetary Damage

Q3			Q2		
State	Total Reported Damages	Complaints	State	Total Reported Damages	Complaints
New York	$52,049,306	1644	Virginia	$55,075,925	1322
California	$37,499,982	2398	California	$52,690,979	2711
Virginia	$27,409,453	1320	New York	$41,045,642	1418
Texas	$25,169,156	1423	Texas	$27,942,988	1864
Washington	$21,986,001	475	North Carolina	$24,783,219	966

From Q3 to Q2, Washington replaced North Carolina in the Top 5 States most affected by financial damage reported to Scambook.

Reported financial damages rose by 26% in New York during the Third Quarter, while reported damages in Virginia fell by approximately 50%.

Scambook Membership by State

1	CA	6	OH
2	FL	7	IL
3	TX	8	GA
4	NY	9	NC
5	PA	10	MI

Scambook Mebership By Gender

46%	Male
54%	Female

CATEGORY ANALYSIS

Who We Are and What We Do

In Q3, Scambook observed the General Consumer category dominate, with 50% of total complaints relating to consumer scams. Our analysts were surprised that Health and Fitness Products made up 10% of complaints in Q3 2012. Scambook plans to track the growth and change of the categories as we move into 2013.

General Consumer	50%
Financial Services	19%
Health and Fitness Products	10%
Text Message / Phone Number	6%
Listing Fraud	5%
Work at Home Programs	3%
Dating Site	2%
Penny Auctions	2%
Dating Services	1%
Dating Profile	1%
Craigslist	1%
Credit Report	<1%
Restaurants	<1%
False Advertising	<1%
Unauthorized Charges	<1%
Other	<1%
Social Network	<1%

HOW SCAMBOOK HELPS

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. If consumer voices aren't being heard, Scambook will amplify them.

Scambook is here for you when:

- **You're unhappy with a product or a service, and the company refuses to issue a refund or even take your calls.**
- **You've been billed by a company and you don't know why, or even who the company is.**
- **You feel ripped off by a company, individual or product and you want to warn others.**
- **You're not sure if that incredible deal or free offer is legitimate or if it's too good to be true.**
- **You want to find out how you can protect yourself and your loved ones from fraud.**

You can search Scambook's exclusive database of over 100,000 consumer complaints and submit your own. No complaint is too small or insignificant. We've helped resolve damages for as little as $5.

Every complaint you submit is reviewed by our Compliance Department, then sorted into categories and grouped with similar complaints. Our Investigation Team works diligently to track down complaint subjects and contact them on your behalf.

Through Scambook Business Resolve, the subject of your complaint can offer you a refund or other compensation. You decide if it resolves your complaint. If you accept the resolution, Scambook sends it to you while keeping your information safe and secure.

We keep you updated about the status of your complaint in your Scambook Dashboard. While you wait for resolution, you can connect with other Scambook users by commenting on company pages or other complaints. You're not alone.

For consumer news, security tips, shopping guides and information about steering clear of the latest fraud schemes, be sure to visit the Scambook Blog: www.scambook.com/blog

> **"With Scambook, people can take responsibility for what happens in their lives and realize there is light at the end of the tunnel when being victimized by companies.**

SCAMBOOK IN ACTION

Scambook Creates A Safe Place For Consumers

Karla and her husband, Eino, are artists living in Pahrump, Nevada. While paying the family bills one day, Karla noticed an alarming $60 charge on her husband's cell phone account. Eino couldn't explain it, so Karla called the phone number associated with the charge. No one answered.

Next, Karla called AT&T. AT&T reviewed Eino's account and discovered that a mobile application company had sent Eino a text message. This text message automatically enrolled him in a monthly subscription service for cell phone wallpaper downloads. Luckily, AT&T refunded Karla's $60. They also placed a block on Eino's account to prevent the app company from re-enrolling him.

But Karla, who is also a community activist, wasn't satisfied. She wanted to spread the word about this unscrupulous company and others who use the same technique to exploit people. Karla emailed all her friends and family. Then, she found Scambook. She submitted a complaint and shared her story with the Scambook community to warn others about this company and their deceptions.

Karla didn't expect to hear from the app company. In fact, Karla forgot about her complaint on Scambook. She was surprised when she received an email a few months later. The app company was working with Scambook to resolve customer complaints. They offered her a refund through Scambook's secure, neutral complaint resolution platform. Karla accepted the refund, but it wasn't about the money anymore. She was thrilled that her complaint on Scambook had helped hold this company accountable for their malicious actions.

"The lack of awareness in consumers is what allows companies to continue with these scams," she said. "With Scambook, people can take responsibility for what happens in their lives and realize there is light at the end of the tunnel when being victimized by companies."

To learn more about Karla and hear other Scambook Stories, watch our videos online at: www.scambook.com/blog

THIRD QUARTER TRENDS

Here's What Affected Consumers the Most in Q3 2012.

Scambook's complaint reports provide an exclusive look at the types of fraud and bad business practices that affect consumers in today's market. By analyzing complaint submission rates, Scambook can determine what's trending, identify patterns and predict future threats. Scambook's insight is new and unique because it comes from the best possible source on fraud: you, our members.

Our database includes over 100,000 unique complaints and that number is constantly rising.

We begin this section by emphasizing the impact of fraud nationwide, with a brief summary of Fraud Factors that increase consumer vulnerability.

Next, we will identify and analyze the Top 3 Complaint Trends on Scambook for Q3 2012:

- **Free Best Buy $1000 Gift Card Texts**
- **HCG Ultra**
- **SurveyCruise.com**

In the following pages, we will describe each of these trends in the words of our members by using direct, unedited quotes from real Scambook complaints. Then, we will present exclusive data charting the trend's reach and complaint submission timeline. We will also include Warning Signs and Safety Tips for each trend.

This section will conclude with General Consumer Tips compiled by our team of anti-fraud experts.

> **"Fraud claims $48 billion in damages every year**

FRAUD FACTORS

Top 5 Reasons Why People Fall For Scams

The Federal Trade Commission estimates that fraud claims $48 billion in damages every year, affecting as many as 30 million Americans every year [i].

Multiple factors contribute to this statistic, including:

Population Density.

Most fraud schemes are traps waiting for unsuspecting consumers, rather than acts targeting specific individuals. Criminals cast a wide net and see what they catch. Places with higher populations will garner more attention from thieves and exploitative businesses.

Age Demographics.

Although anyone can fall victim to fraud, senior citizens are usually affected in greater numbers than younger generations. The elderly tend to be more trusting, more easily intimidated and less familiar with technology such as the Internet. Crimes of identity theft are an exception, however. According to the FTC, 31% of identity theft victims in 2011 were age 29 or younger [i].

Internet Usage.

This is why younger people compose a majority of identity theft victims. People who spend more time on the Internet give criminals more opportunities to steal their private information. Internet users are also more likely to be ripped off by fake online retailers or bogus auctions.

Language Barriers.

Non-English speakers are more likely to be exploited because they won't be able to spot the warning signs of fraud. They may also be less likely to seek outside help and take action when they become victimized.

Economic Hardship.

Everyone loves a bargain, but saving money becomes even more important during hard times. Being too eager for a deal, a new job or a payday loan may cloud a victim's judgment and make them more vulnerable. Fake job schemes, such as illegitimate Secret Shopping and Work at Home systems, also thrive whenever consumers need extra cash.

In Q3 2012, the leading fraud trends focused around Internet Usage and Economic Hardship to exploit consumers via mobile text messaging, social media and misleading free offers.

Top Trend: Free Best Buy $1000 Gift Card Texts

A spam text message disguised as an official offer from Best Buy that attempts to gain the recipient's private or financial information.

- In Q3, Complaint Reports Rose 305% for this trend.
- 897 Complaints
- Total Reported Damages $4,703,633.26
- #1 for Consumer Impact, #3 for Site Pageviews

Summary

Also known as "smishing," these spam text messages direct recipients to redeem a prize (a Free Best Buy $1000 Gift Card) for a contest they didn't enter. The messages originate from a variety of different phone numbers, however, the message instructions do not vary significantly. BestBuyWin.net, BestBuyWin.mobi and the other websites associated with these smishing texts are always a clever spoof of the real BestBuy.com website.

By mimicking Best Buy's corporate branding, websites like BestBuyWin.net and BestBuyWin.mobi can mislead users into believing that the gift card offer is affiliated with or endorsed by Best Buy. Users are eager to redeem their $1000 gift, but to do so, they must participate in a rewards program by purchasing costly memberships and special offers. These sites will also share the user's information with third-party marketing companies.

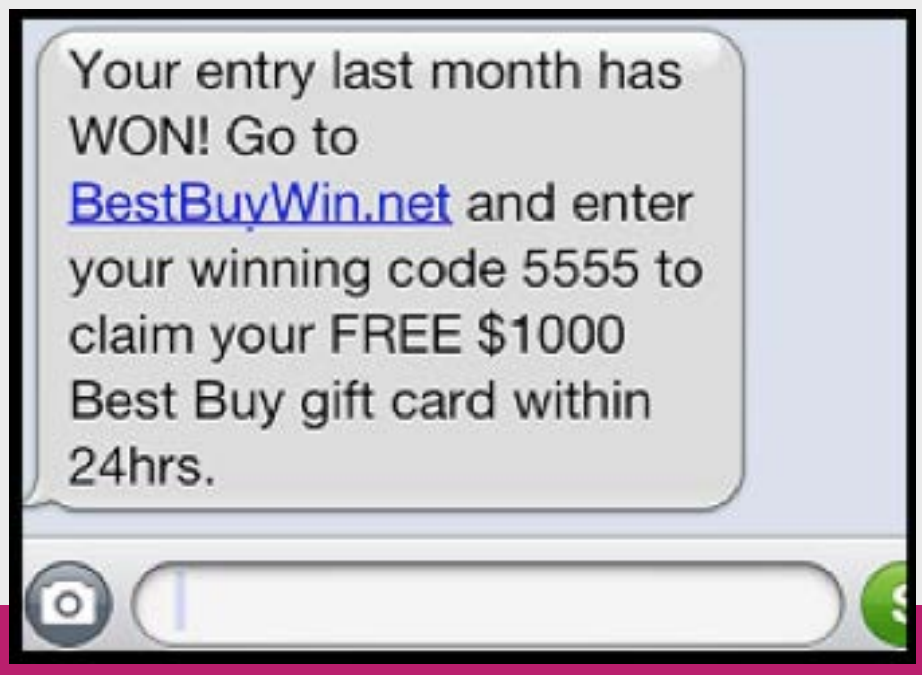
Scambook reached out to Best Buy for an official statement:

"Some customers may have recently received a text message indicating that they won a $1,000 Best Buy gift card. It prompted customers to visit a third-party site set-up to look like our brands. This message did not originate from Best Buy or Geek Squad and was not a result of a breach of our customer information.

"We have taken a number of steps, including legal action, to address these types of scams. In these rare instances [when customers complain], we individually respond to customers and apologize for any frustration or inconvenience and work to resolve immediately."

Our research shows that Free Best Buy $1000 Gift Card Texts have targeted consumers every quarter with increasing numbers. Based on complaint submission rate and site analytics, Scambook estimates that 84,000 people nationwide received these text messages near the end of Q3 2012. This attack has continued into Q4.

We predict that an additional 100,000 cell phone users will receive a Free Best Buy $1000 Gift Card Text by mid-November, corresponding with the holiday retail season.



Statistical Visualization:

Free Best Buy $1000 Gift Card Texts

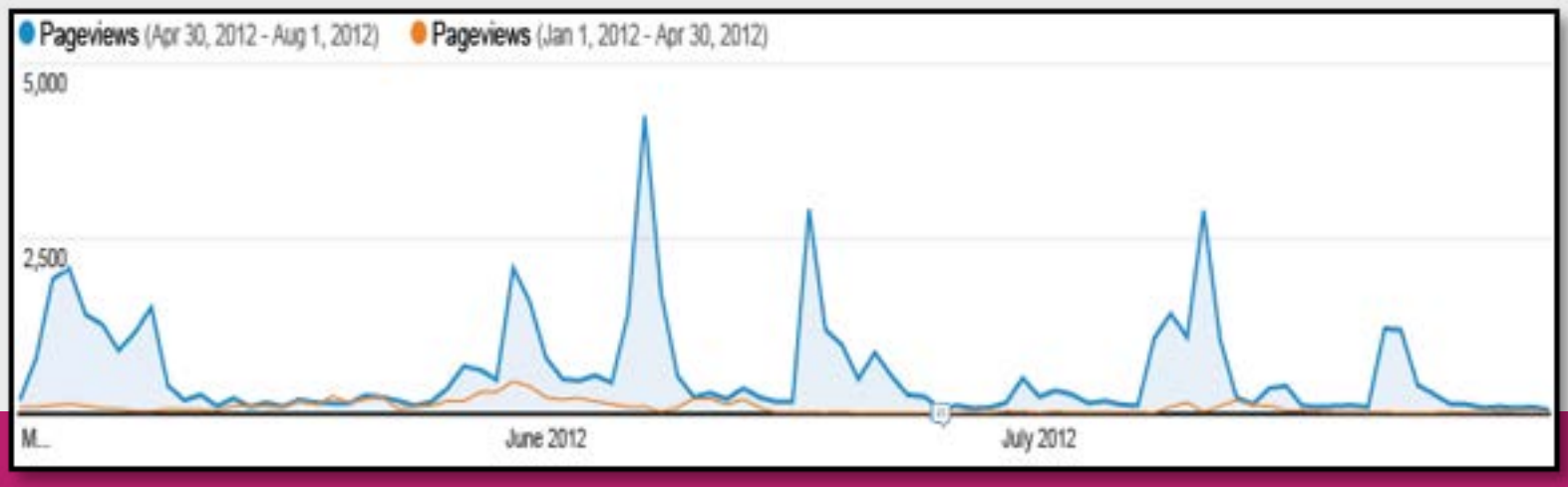
Location Mapping

Range of effect, Free Best Buy $1000 Gift Card Texts. Cell phone users all across the United States have received these unwanted spam text messages, with greater concentration on the coasts and densely populated urban areas. Data Source: Scambook.com

Q3 Activity Level Shows A Dramatic Spike In September

Our analysis shows that Free Best Buy $1000 Gift Card Texts follow a consistent wave-like pattern. Activity levels for Free Best Buy $1000 Gift Card Texts were low for most of Q3, then spiked dramatically in September.

Q1 and Q2 Activity Levels Show Two Earlier Waves



Data Source: Scambook.com

User Comments:

What Scambook Users Are Saying About Free Best Buy $1000 Gift Card Texts

"Received a text message on my cell phone from 909-837-7749. The text states: your entry last month won. Go to bestbuywin.net. and enter your winning code 5555 to claim your free $1000.Best Buy gift card within 24 hrs. I never entered any contest and never give out my cell number, I always list my home number on every form I complete as to not receive unwanted text messages. My cell number is reserved for friends and family only.How are they getting my cell number? [sic]"

Actual Scambook User

“I recieved a text message at 5am this morning saying your entry last month has WON! Go to BestBuy-Win.net & enter your winning code 5555 to claim your Free $1000 Best Buy gift card within 24hrs. I have not entered any contest & do not appreciate spam being sent to my phone. [sic]”

Actual Scambook User

“Got text message stating that I won $1000 gift card from Best Buy and to click on link to claim. I never entered a contest and haven’t shopped there in a year. Had to be scam! Just wondering how they got my cell #!?![sic]”

Actual Scambook User

“http://bestbuywinners.mobi/ sent a text message to my cell phone stating I won a $1000 Best Buy gift card. This is a fraud and I am not sure how they got my cell number. I do not shop at Best Buy and certainly would not give them my phone number, especially a cell phone number. [sic]” [source]

Actual Scambook User

Warning Signs and Safety:

Free Best Buy $1000 Gift Card Texts

Look for the following warning signs and use the following safety tips to avoid being ripped off or defrauded by Free Best Buy $1000 Gift Card Texts.

If you receive a text message from an unknown number, watch out for these warning signs:

- **"You're a winner!!!" But you never entered any contests and you need to pay money, fill out surveys or sign up for a special offer to redeem your prize. If something is legitimately free, you won't need to take these steps. Additionally, companies like Best Buy won't contact you out of the blue via text message.**
- **"Visit BestBuyWin.net." Beware websites that spoof legitimate companies. If Best Buy was involved with this offer, they would direct you to BestBuy.com, not another site.**
- **"Reply with your phone number, email, password or PIN." A legitimate company will never request your personal information in an unsolicited text message.**
- **"Act NOW! You have 24hrs." Fraudulent schemes often attract victims by creating a false sense of urgency and pressuring the victim to act before these deals expire.**

Spotted one or more of these red flags? Here's what Scambook recommends:

- **Don't reply. The perpetrators of these smishing schemes use an algorithm that selects phone numbers at random, which means they don't know which numbers are active. If you text back, even to say UNSUBSCRIBE, you're letting them know that your number works and you're likely to receive even more spam.**
- **Don't redeem your "free prize." It's tempting, but "free" gift card offers from sites like BestBuyWin.net are extremely misleading. These sites require you to join paid reward programs and recruit friends to do the same, then share your personal and financial information with third-parties.**
- **Contact your wireless provider. Take a screen shot or a photo of the text message to report to your cell phone company. If you continue to receive these smishing texts, find out how you can alter your cell phone plan and block text messages.**
- **Contact the company represented in the text. If you're still not sure whether a text message offer is legitimate, go online and contact the company represented in the offer. This will also help them become aware of the problem and address it.**

We also encourage anyone who receives these text messages to report the incident on Scambook.

Top Trend: HCG Ultra

A misleading diet product with alleged connections to phishing and social media hacking.

- In Q3, Complaint Reports Rose 91% for this trend.
- 248 Complaints
- Total Reported Damages $$1,038,092.58
- #2 for Consumer Impact, #1 for Site Pageviews

SUMMARY

HCG Ultra is a supplement marketed to dieters in drops. HCG, which stands for human chorionic gonadotropin, is a hormone found in the urine of pregnant women. Promoters say that HCG suppresses hunger and boosts metabolism. Dieters on HCG plans are instructed to follow a strict 500 calorie diet for 45 days while injecting HCG or taking HCG oral drops such as HCG Ultra. Manufacturers claim that the product delivers incredible results, such as losing 20 pounds in 20 days.

WebMD cites numerous studies that dispute this, noting that "scientific studies have demonstrated that HCG injections do not cause weight loss."[ii] Experts also point out that HCG hasn't been approved by the FDA and evidence suggests that HCG drops, such as HCG Ultra, contain such a small percentage of the actual hormone that the drops are essentially a placebo. When users do lose weight on an HCG program, experts believe this is due to the 500 calorie diet restriction that accompanies the supplement program, rather than the HCG itself.

HCG Ultra is also connected to phishing (spam email designed to steal the recipient's private information) and social media hacking. Scambook members allege that they ordered the product after a friend emailed them or sent them a link via Facebook, directing them to a commercial website mimicking Fox News. Members later discovered that the person who sent them the link was hacked. Scambook members also report difficulties contacting HCG Ultra customer service and obtaining refunds.

Our data shows that HCG Ultra was a new trend that appeared at the end of Q2, gaining momentum in July and August before tapering out in September.

Scientific studies have demonstrated that HCG injections do not cause weight loss.

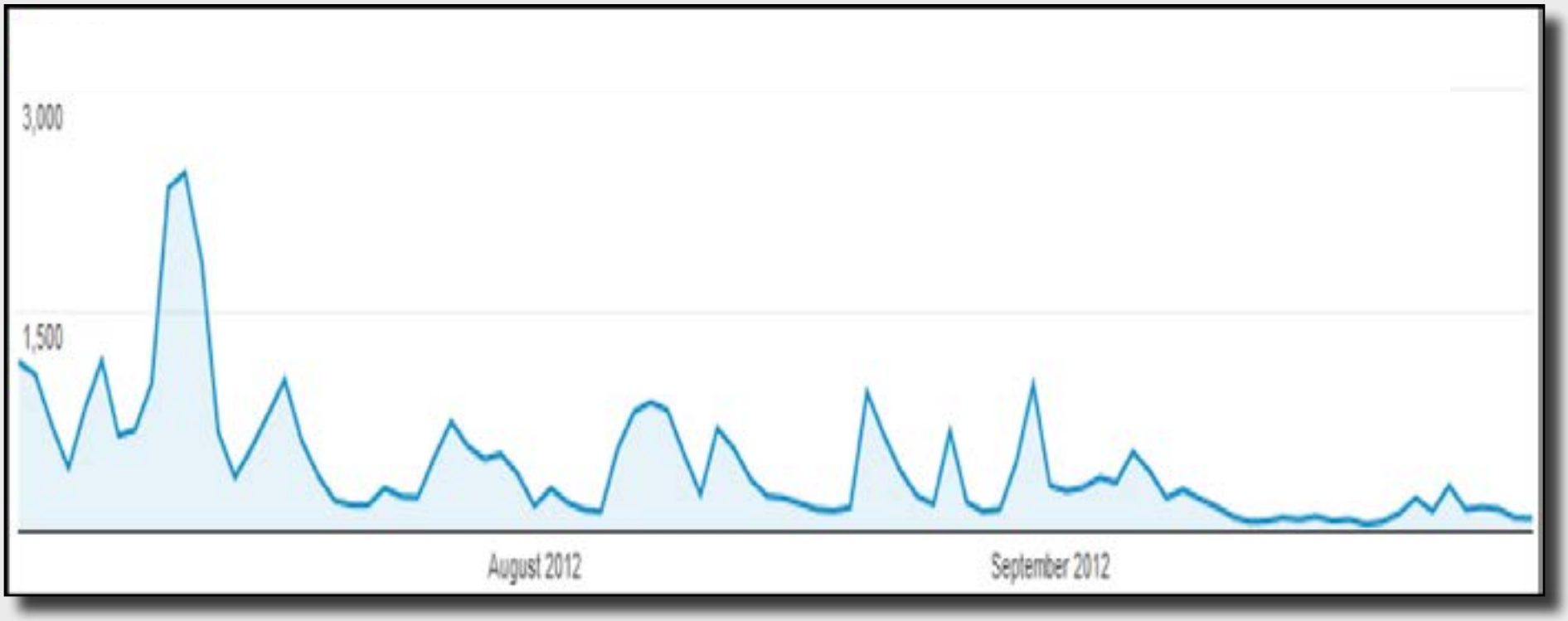
Statistical Visualization:

HCG Ultra

Location Mapping

Range of effect, HCG Ultra. As one of the Top 3 Complaint Trends for Q3 2012, Scambook received complaints about HCG Ultra from all over the world with the greatest concentration in the United States.

Q3 Activity Level Shows An Increase in Activity



Complaints about HCG Ultra first appeared as a trend in late Q2 2012, gaining momentum at the beginning of Q3 and tapering off in September.

Data Source: Scambook.com

User Comments:

What Scambook Users Are Saying About HCG Ultra

“I saw an ad on the net and supposedly a woman who works for Fox had rave revues about this. It seemed that all you were to have to do was take the product and lose weight. They failed to mention you had to go on a 500 calorie diet! Anybody can lose if they’re on a 500 calorie diet!! [sic]”

Actual Scambook User

“A Serbian IP hacked into my mail account (I have since changed all of my passwords and security questions), and sent an email to every one of my contacts with no subject and only a link in the body. The link was a redirect page hosted by some rench martial arts dojo (WTF?) that sent visitors to a page that promoted HCG Ultra’s product. This is fraudulent and horrendously unethical business practice. Not only that, but their product has been made illegal by the FDA for any OTC sale for any purpose. This company, and all affiliated organizations (including whoever hacked me), needs to be shut down before it can cause any more damage. [sic]”

Actual Scambook User

“hacked my facebook account with a “post” I supposedly made stating that I took the product and lost weight. even included a comment from me to validate the “post”. I then got a warning from facebook that my account had been compromised and my account had been suspended. [sic]”

Actual Scambook User

"We saw a Fox News reporter online tried the HCG drops and said they were a success. We then ordered 2 bottles of the HCG drops on 9/3 and received them on 9/10, no receipt in box or anything of the sort. So we found that rather strange. But I tried them and I saw NO RESULTS so we were attempting to send them back and get our money back. The website we ordered from is GONE and NO phone number or address besides the Fullfilment center, and they had the 15 day money back GUARENTEED! This is VERY FRUSTRATING! [sic]"

Actual Scambook User

Warning Signs and Safety:

Free Best Buy $1000 Gift Card Texts

Look for the following warning signs and use the following safety tips to avoid being ripped off or defrauded by HCG Ultra.

If you receive an email or a social media message promoting a weight loss product like HCG Ultra, look for these warning signs:

- **No email subject, no text, just a link. Often, emails sent from hacked accounts include nothing more than an ambiguous link. If you receive a suspicious message from your friend or family member, reach out to them directly and ask about the email.**
- **A page mimicking Fox News, CNN, NBC or another news site hosted at a different domain. Although the HCG Ultra "news article" looks very legitimate, it's not hosted at foxnews.com.**
- **Endless redirection. If you click on an email or social media link and it keeps automatically redirecting you to different sites you've never heard of, it could be fraudulent.**
- **Strange social media activity. Are you seeing Facebook posts about weight loss from your skinniest friend? Do you have an older relative who always types in complete sentences, and suddenly he or she is using Internet slang and emoticons? Any "out of character" social media activity may indicate that your acquaintance has been hacked. Don't click the links they're sending you.**

Spotted one or more of these red flags? Here's what Scambook recommends:

- **Don't click. If someone posts on your Facebook timeline about HCG Ultra Drops, or you receive a link to that faux Fox News page, we urge you to ignore it. Any time you receive a suspicious message from a friend or family member, such as an odd email link with no subject or description (or a subject/description that doesn't sound like something your friend would write), contact the sender and let them know that they may have been hacked. Delete the email and report it on Scambook.**
- **Contact your friend or family member. The person who sent you the phishing email may not be aware that they've been hacked. Don't reply to their suspicious email, but send them an IM or call them and ask about it.**
- **Review your online security. Now's the time to make sure you haven't been hacked, too.**

We also encourage anyone who receives a message about HCG Ultra to report the incident on Scambook.

Top Trend: SurveyCruise.com

A telemarketing call that targets mobile phone users and tries to obtain personal information through a free cruise offer.

- In Q3, Complaint Reports Rose 15% for this trend.
- 455 Complaints
- Total Reported Damages $$7,966,233.86
- #3 for Consumer Impact, #2 for Site Pageviews

SUMMARY

SurveyCruise.com is a website associated with a telemarketing call that targets cell phone users in the United States, the UK and Canada. The calls originate from a variety of different phone numbers, begin with a prerecorded message and then prompt the recipient to answer a series of questions. The recipient is told that he or she will receive a free cruise in exchange for their participation. The recipient is directed to SurveyCruise.com to redeem their prize.

SurveyCruise.com appears to be operated by the United Public Opinion Group. The website states that the user's survey answers are "analyzed by companies to determine consumer market trends," and that "you and or[sic] your household are agreeing to be contacted by us to participate in 10-25 question surveys or opinion polls periodically throughout the year."

Scambook users who attempt to redeem their cruise tickets report that they experience difficulty with the website and never receive their prize. In some instances, they receive calls for additional surveys, despite requests to remove their number from the organization's list.

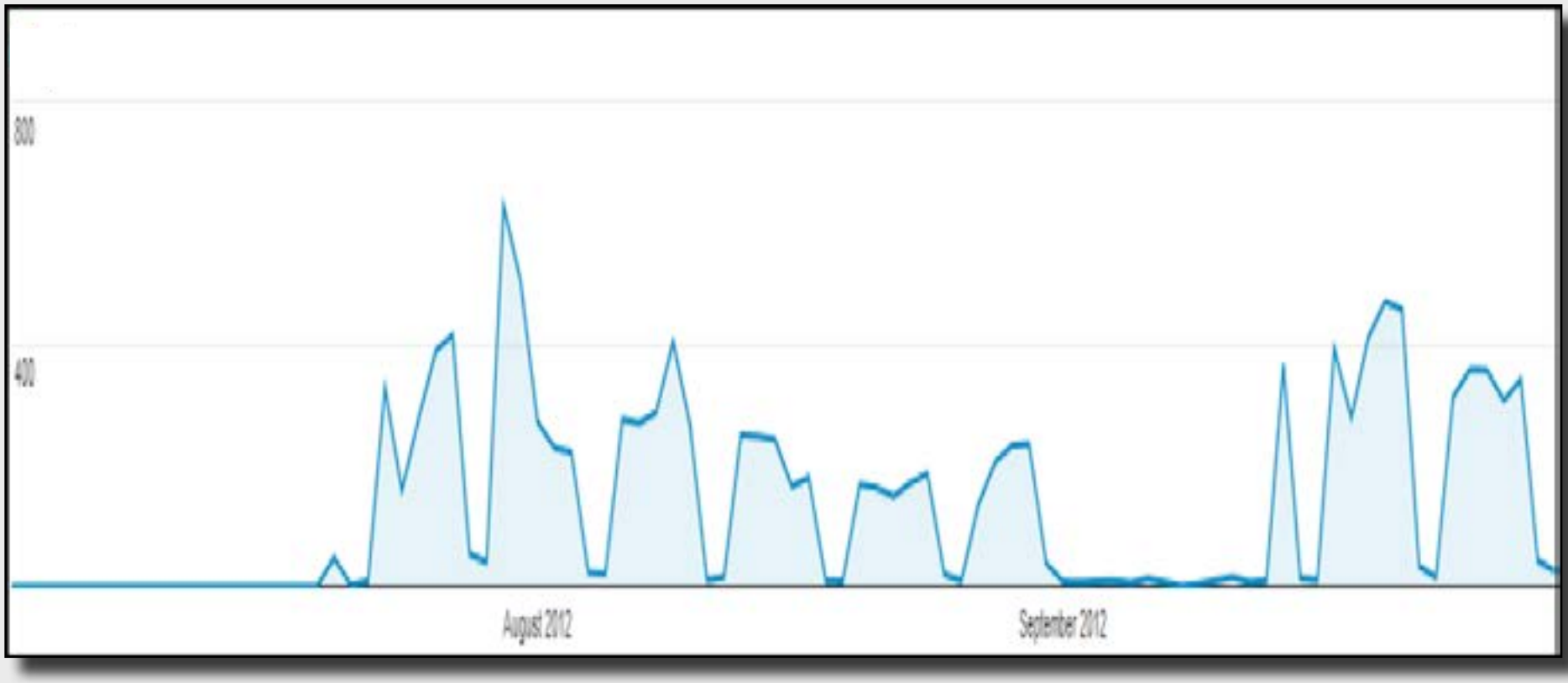
Statistical Visualization:

HCG Ultra

Location Mapping

Range of effect, SurveyCruise.com. Our complaint submission data shows that SurveyCruise.com targeted cell phone owners in the United States with distribution corresponding to population dispersal. Data Source: Scambook.com

Q3 Activity Level Shows An Increase in Activity



Complaints about SurveyCruise.com spiked in August, then continued with a steady report pattern. We observed a brief lull in early September before another surge of activity continuing into Q4. Data Source: Scambook.com

User Comments:

What Scambook Users Are Saying About SurveyCrusie.com

"Surveycruise.com called me on my cell phone and advised me to take this survey and I would receive an all expense paid cruise for me in the Bahamas and beyond. They asked personal questions about myself and family; plus was I a homeowner. I thought it was to good to be true. Next, they transferred me to an answering service. How they got my number is disgusting I use that phone number for work and personal family only. [sic]"

Actual Scambook User

"I was just called by an automated service for this company,at my place of business, answer their questions, recieve 2 tickets for a Bahama cruise. Surprise!!! The website to confirm the tickets does not exist!!!!! [sic]"

Actual Scambook User

“I was also called by said company asking my education level, age, if we had a septic tank and if anyone in the family has diabetes; I was told I won 2 free tickets for a cruise to the Bahamas, that a travel agent would be calling me and to log onto their website. It's bogus[sic] "

Actual Scambook User

"Was called (at random) by an automated survey (united public opinion group) asking questions about my education level, and certain medical issues I may/may not have. It was in exchange for a cruise trip for two, for free. After the survey was completed I was directed to a live operator who (sounded indian) asked for my correct phone number and zip code which was supposed to be used to log in to their company website (www.surveycruise.com) to claim a reward. It (of course) didn't work and after a number of attempts I was directed to a page for contacting them if I was having technical difficulties, and after filling out the information and hitting 'send', it automatically redirected to an 'error' page. [sic]"

Warning Signs and Safety:

SurveyCruise.com

Look for the following warning signs and use the following safety tips to avoid being ripped off or defrauded by SurveyCruise.com.

If you receive an unsolicited phone call from a number you don't recognize, look for these warning signs:

- **Is it a prerecorded message? Telemarketing and fraudulent phone calls often use prerecorded messages. Although many prerecorded messages will transfer you to a live operator, it's still a suspicious sign.**
- **Is the caller telling you that you've won a prize or a contest you didn't enter? Always be on guard whenever you've won a free prize, especially when you're not aware that you entered any contest. Watch out for "free" prizes and special offers that require some action on your part -- whether it's joining a subscription rewards program, answering survey questions or providing your credit card information. These deals are usually too good to be true.**
- **Is the caller asking for your personal information? Be wary of unsolicited calls that request your personal information, especially if you don't recognize the number.**
- **Is the caller asking for your financial information? Remember, legitimate organizations won't call you out of the blue to ask for your credit card number or other financial information.**

Spotted one or more of these red flags? Here's what Scambook recommends:

- **Don't give any personal information. If the caller represents a legitimate company, get the company's information as well as the name and extension of the caller's supervisor. Then, research the company on Scambook and other consumer safety websites. If you discover that the organization (and their special offer) is real, you can always call back later.**
- **Record the number, as well as any relevant details such as the name of the person you spoke to, or some keywords from the prerecorded message. Call your mobile phone company and let them know you're being harassed. They may be able to block the number from calling you.**
- **Keep an eye on your phone bill. Scambook recommends that users who receive suspicious calls pay extra careful attention to their monthly bills. If you see any charges you don't recognize, alert your phone company right away and file a dispute if necessary.**

We also encourage anyone who receives a call from SurveyCruise.com to report the incident on Scambook.

General Consumer Safety Tips

- 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
- 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.
- 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.
- 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.
- 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.
- 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.

ADDITIONAL RESOURCES

Previous 2012 Quarterly Reports

Scambook's First Quarter 2012 and Second Quarter 2012 Industry Reports are available online.

Download our Q1 Report here:
http://www.scambook.com/press/scambook_market_report_q1_2012

Download our Q2 Report here:
http://www.scambook.com/press/scambook_industry_report_q2_2012

Press Contact

For more information about Scambook or to request supplemental materials, please contact:

5900 Wilshire Blvd 21st Floor
Los Angeles CA, 90036
press@scambook.com
1-877-966-2278 ext. 4896

External Links

[i] FTC.org, Consumer Sentinel February 2012. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf

[ii] WebMD.com, The Truth About HCG for Weight Loss. http://www.webmd.com/diet/features/truth-about-hcg-for-weight-loss