THREAT ANALYSIS

eCommerce Fraud on the Rise

How Scam Merchants are Affecting Financial Institutions, Retailers and Brand Trust

September 2023

RESEARCH
Table of Contents

Executive Summary 3
   Cost to Financial Institutions 3
   Cost to Retailers 5
   Cost to Consumers 6
Identification 8
   Scamming Methodology 8
   Template Sites 9
      Website Formats 10
      Social Media Links on Contact Pages 10
      Alternative Names on Credit Statements 11
   Contact Email Addresses 12
Brand Misuse 14
   Site Content Rotation 16
   Product Image Theft 18
   Sending Incorrect Merchandise 20
China Connection 20
   Shoesdiscounting.favorablebxs[.]com 21
   Fictional Address 22
      usdiscountsing[.]com 23
   Scam Sites for Sale on Chinese Platforms 25
   Chinese Language Site Messages 26
US Connections 27
   Postal Service 27
      buydiscountusps[.]com 27
      uspsstamp[.]co 29
   Other Sites 30
Conclusion 31
Appendix A: Scam Site Format Examples 32
Appendix B: Scam Site Email Addresses 33
Appendix C: Company Names on Bank Statements 37
   AP buygoodsing Singapore 37
   Helipay Lovetheshops 40

DISCLAIMER:
The reporting contained herein from the Nisos research organization consists of analysis reflecting assessments of probability and levels of confidence and should not necessarily be construed as fact. All content is provided on an as-is basis and does not constitute professional advice, and its accuracy reflects the reliability, timeliness, authority, and relevancy of the sourcing underlying those analytic assessments.
Executive Summary

Financial institutions and retail businesses face increasing fiscal and reputational harm from scamming networks operating fraudulent online stores. Organized criminals’ use of template sites to quickly create thousands of fake stores enables them to attract victims of all interests effectively. Victims’ attempts for reparation may ultimately rely on financial institutions’ efforts or reimbursement, resulting in financial losses or damage to their reputations if victims are unsatisfied with their support.

Nisos researchers identified a China-associated scam network operating likely thousands of fraudulent online stores that pose as major brands and do not provide the purchased merchandise. These sites attract victims by offering highly discounted products and formatting their pages to include logos and images from the brand’s official web pages. While most victims did not receive any products, some received cheap goods in place of large electronics or other expensive items. By not receiving the correct products, most victims were not eligible for the fraudulent online stores’ return policies, and the sites’ regularly changing contact information negated attempts at reimbursement.

The websites involved in this scam network utilized multiple identical Chinese-language template sites designed to build online stores quickly. In addition to products and images used to pose as a legitimate representative of popular brands, the contact information for these pages included a rotating list of email addresses. Site contact information, products, and branding were regularly updated, possibly in an attempt to confuse or deter investigative action, particularly if the website no longer appeared similar to when the victim first made their purchase.

Cost to Financial Institutions

Victims of this scam are often left with financial institutions as their only chance to regain their money, putting pressure on banks to take a loss to keep their clients happy. The inability of a financial institution to refund the customer — for whatever reason — could ultimately impact its customers’ trust and negatively affect its reputation. Similarly, victims’ frustration in this situation could be directed towards the big brand stores from which they believed they were purchasing merchandise. Some may hold these brands ultimately responsible for their losses for allowing these types of imposters to prey on shoppers, particularly if they are unaware of the prevalence of these scams.

This scam also costs financial institutions valuable time and resources, as victims are often left with no other avenue than to contact their bank and attempt to stop or refund the payment. These scams frustrate direct interactions with the fraudulent sites through non-responses, constantly changing email addresses and debilitating refund/return policies. The ultimate lack of satisfactory resolution for the victim and the steps required to protect their financial information following these purchases could cause frustration with and reputational damage towards the banking institution by the customer.
Recommendations for Financial Institutions

Nisos recommends financial institution investigators look for specific indicators of fraudulent companies when researching fraud perpetrated against customers, which include the following steps:

1. Collect any contact information available on the website associated with the company (i.e., its company name, phone number, email address, physical address, and return address).

2. Search online for these pieces of information — with and without quotes around the search terms — in order to identify similar websites and patterns.

3. If product prices listed on these sites seem too good to be true, they probably are. This could suggest that actual merchandise is not sold on these sites. A comparison of these products with other online sellers can create a strong baseline for reasonable retail pricing.

4. Verify if the addresses listed for the companies are physical locations or virtual mailboxes through basic online searches and using tools such as Google Maps.

5. Consider interacting with the website’s support phone number. Scam sites will often rely on what customer service representatives refer to as “third-party customer service centers” and will be unwilling to provide any identifying information about the questionable website or the call center itself. Sometimes, these numbers are randomly selected and belong to unassociated individuals.

---

1https://www.scamwatcher.com/scam/view/631676

© Nisos - The Managed Intelligence Company® | eCommerce Fraud on the Rise
Page 4
6. Review the documentation or emails provided by the suspected fraudulent merchant to the financial institutions for inconsistencies with the alleged charges, including alternative company names appearing on the charges.

Cost to Retailers

According to the FBI, brand impersonation costs U.S. businesses over $2 billion annually, with every $1 of fraud costing victim merchants $3.85.\(^2\) Consumer victims may ultimately hold the impersonated retail brands responsible for the losses they experience. Big retail brands could be blamed for allowing these imposters to prey on consumers through alleged inaction or lack of remediation.

![Graphic 2: Example of site brandnewsell[.]com associated with template site cdn.staticsoe[.]com impersonating Lowe’s, as of 13 June 2023.](image)

Recommendations for Retailers

Nisos recommends retail investigators look for specific indicators to stay ahead of fraud:

1. Monitor registrars and DNS providers for newly registered domains that could create confusion with the brand.

2. When fraudulent sites are discovered, identify ISPs, web hosting providers, DNS providers, registrars, registrants, and owners of any hijacked web properties that can assist with a takedown.

\(^3\)https://brandnewsell[.]com/
3. Work with local Law Enforcement or the relevant CERT to inform them of any crime and facilitate any legal action.

4. Monitor for fraudulent mobile apps that appear as well-respected brands, Criminals use such tools as a trojan horse to give them root-level access to steal data stored on devices.

5. Monitor social media and the dark web for company mentions. Fraudsters will use the dark corners of the web to sell stolen credentials and payment card data, launder stolen merchandise, and monetize their crime.

6. Monitor for criminals impersonating your employees. Fake profiles for executives, partners, or suppliers can be signs of a larger scheme.

Cost to Consumers

Fraud networks, like the one outlined in this report, are just part of a growing criminal ecosystem that cost Americans nearly $8.8 Billion in 2022.\(^4\) Victims lose significant finances to fraudulent online stores by purchasing undelivered products and the often high cost of shipping attached to the sale. Many of these sites contain caveats that products cannot be refunded unless the product — which most of the time they never receive — is returned and additional shipping paid. Those who receive a cheap item in place of the ordered merchandise are not able to return that in place of what they should have received.

Recommendations for Consumers

Consumers must be vigilant and discerning to avoid becoming victims of fake eCommerce sites. According to ACAMS, here are some indicators consumers can use to identify fraudulent eCommerce sites:\(^5\)

1. Different sellers using the same photos or posting photos of merchandise with the same background.

2. Sellers using stock retail photos.

3. The item price is significantly less than the price of other sellers on the marketplace or below manufacturers' cost.

4. Advertisements include language such as: “like new;” “new in box” or “NIB;” “new with tags” or “NWT;” “unopened;” “taking orders [for product];” “DM for orders or size;” and “factory sealed.”

5. The company’s website is not functioning or lacks accurate or updated information.

6. The company’s address is associated with land with no building, a warehouse with no sign, or a building without the company's name/storefront.

\(^5\)https://www.acams.org/en/media/document/29436
7. The company’s website does not allow direct purchases, indicating consumers must first contact the retailer.

8. Website URLs or usernames contain variations such as: “Pawn;” “Flea Market;” “below sale;” “wholesale;” or “wholesale OTC.”
Identification

Our research into this network demonstrates how the average shopper could easily fall victim to this scam. In March 2023, a Nisos analyst researched playground equipment to purchase for their children. After identifying a specific model they wanted to purchase, the analyst noticed the equipment posted for a similar price on multiple big brand sites. However, one site, vokyn[.]com, listed the same equipment for less than half the price.

The analyst identified the contact information for vokyn[.]com present on dozens of other similarly structured sites, many of which claimed to represent big brands. The analyst ultimately decided against any purchases from these sites. However, these sites are effective at attracting victims, judging from the number of associated scam complaints.

Analyst Note

Hundreds of additional sites exist that claim similar email addresses, physical addresses, phone numbers, or use the same techniques and templates as those provided in this overview. We focused our examples below to sites associated with a content delivery network (CDN) connecting to specific similar template sites to limit the scope and concisely present patterns.

Scamming Methodology

This particular scamming network used the following methods to establish associated fraudulent online stores. Other scamming networks beyond the scope of this report likely adopt these practices in whole or in part.

1. **Creating Fake Digital Stores:** The overseeing network establishes multiple fraudulent online stores that are quickly built using pre-established template sites. These sites pose as known brands and regularly contain contact information associated with actual brand locations.

2. **Attracting Customers:** The fraudulent online stores claim to offer significant discounts on official brand merchandise. Product images are stolen from official brand websites or independent merchants.

3. **Failing to Send Merchandise:** Victims of the scam often do not receive any products from the site. Those that do receive a product are sent cheap merchandise such as socks, hats, scarfs, or wallets. Company names not associated with the site or the advertised brand appear on the victim’s credit card statement.

4. **Contact with Site Representatives:** Victims’ attempts to obtain a refund or return the incorrect merchandise to the site are hindered by complicated policies, high shipping costs, and unresponsive contact emails.

5. **Rotating Contact Information and Site Content:** The sites regularly rotate or remove email addresses listed on their home and contact pages. Sites are sometimes repurposed to represent alternative brands.
6. **Disappearance and Creation of Sites:** The fraudulent online stores have a short lifespan and are often taken offline by administrators within two to four months. The network continues its process of creating new sites associated with the same templates, regularly creating similar sites through this process — i.e. creating identical sites stampbuyhome[.]com and stampbuyhome[.]co on different days.

**Template Sites**

Fraudulent online storefronts in the scamming network are linked to multiple Chinese-language template sites that allow for users to quickly produce an online shop. These template sites included staticsoe[.]com, staticsyy[.]com, ymcart[.]com, and oemcartapp[.]com, although many other active and now-inactive template sites were also associated with these fraudulent online stores.
Website Formats
Online stores using the template sites generally have the following features:

- A banner across the top advertising sale prices or delivery deals.
- Random pop-ups advertising sale prices in the bottom left corner.
- Limited or empty information on their contact page.

Many of the sites also claimed their copyright association with SHOP INC, although the sites also claimed different organizations. [See Appendix A for additional examples of site format features]

The majority of these sites listed addresses and phone numbers attributed to the companies they were impersonating, while others listed likely randomly selected numbers belonging to unsuspecting victims. These included phone numbers and home addresses attributed to US citizens unaffiliated with the scam.

Social Media Links on Contact Pages
Many of the fraudulent online stores contained icons for popular social media platforms, likely as a facade to appear more legitimate to potential customers. These icons only redirected to the front page of the social media platform or to the fraudulent online store site.
Alternative Names on Credit Statements

Victims identified alternative company names alongside the charges on their credit card statements. We identified these companies — including AP buygoodsing Singapore and Helipay Lovetheshops — as likely run by individuals supporting the China-centered scam network. [See Appendix C for additional information on these companies and their links to China]
Graphics 7 and 8: Examples of AP buygoodsing Singapore (top) and Helipay Lovetheshops (bottom) appearing on credit card statements following purchases from scam sites.11 12

Contact Email Addresses

We identified the following email addresses listed on multiple of the fraudulent online stores. We observed instances where an email address was present on one site but was rotated to another email address at a later time. Often, the original contact email address remained visible in the page source

11https://www.scamwatcher[.]com/scam/view/578668
12https://www.truffeonline[.]com/scam/view/589657
even after the email address was replaced. This pattern helped identify multiple email addresses through a single website.

- Website xhfadacai[.]com was historically associated with four email addresses, with pamela@sdhbell@gmail[.]com and sarkilsat@gmail[.]com present on the site’s contact page on 28 April 2023, previous email address jmservicefor@gmail[.]com visible in its page source, and prior email address behnekeiofdr@gmail[.]com identified in a complaint on the Better Business Bureau’s (BBB) website.\(^{13}\) \(^{14}\) \(^{15}\)

- Website lasdirectsales[.]shop changed its contact email address from jmservicefor@gmail[.]com to liudang67qq@gmail[.]com between March and April 2023. As of early June, the site no longer listed any contact email address.\(^{16}\)

- Website dreamingtoning[.]com listed email address liudang67qq@gmail[.]com on its contact page as of 28 April 2023, while its page source listed email address a1127040642@gmail[.]com.\(^{17}\)

[See Appendix B for additional information on email addresses]

\(^{13}\)https://xhfadacai[.]com/pages/Contact-Us
\(^{14}\)view-source:https://xhfadacai[.]com/pages/Contact-Us
\(^{15}\)https://www.bbb[.]org/scamtracker/lookupscam/704734
\(^{16}\)https://www.lasdirectsales[.]shop/pages/Contact-Us
\(^{17}\)https://dreamingtoning[.]com/pages/Contact-Us_a494d46b
\(^{18}\)view-source:https://dreamingtoning[.]com/pages/Contact-Us_a494d46b

© Nisos - The Managed Intelligence Company® | eCommerce Fraud on the Rise
Page 13
Brand Misuse

Nisos identified these email addresses listed as contact information on sites posing as major and minor brands, including Walmart, Lowe’s, Costco, Skechers, Nike, LL Bean, Wayfair, Mamas & Papas, Oroton, the US Postal Service, and many others.

Graphic 10: Examples of multiple stores posing as Walmart.

Graphic 11: Example of website posing as Lowe’s.19

19https://www.dreamtoning[]com/pages/Contact-Us_a494d46b
Graphic 12: Example of website posing as Skechers.  

Graphic 13: Example of website posing as Nike.  

Graphic 14: Example of website posing as Mamas and Papas.  

Graphic 15: Example of website posing as Oroton.  

© Nisos - The Managed Intelligence Company® | eCommerce Fraud on the Rise
Site Content Rotation

In addition to rotating email addresses, these sites are regularly repurposed to pose as different brands. These sites often use company logo favicons, which sometimes remains following a site’s restructure. Google results for website sikags[.]com as of 19 May 2023 showed the Walmart favicon alongside the

---

24 https://www.lbhot[.]shop/
25 https://onlineboots[.]shop/pages/Contact-Us
26 https://www.costco[.]com/warehouse-locations/victorville-ca-1010.html
search result. However, the actual site no longer claimed any direct association with Walmart at that time.

<table>
<thead>
<tr>
<th>sikags.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Us</td>
</tr>
<tr>
<td>Customer Service: <a href="mailto:pamelagsdbell@gmail.com">pamelagsdbell@gmail.com</a>. Attention: Please ensure your account email is right so that you will receive an order confirmation after ...</td>
</tr>
</tbody>
</table>

Fraudulent online store loungespin[.]com posed as an online store called Atop with contact email hello@atop[.]pet as of 9 June 2023. However, this site previously displayed the name FREEXVIDOES and contact email address hello@freexvidoes[.]com as of 19 April 2023. This likely indicates that an earlier repurposing of the domain overlooked adjusting the title and contact information. The banner on the site also included a grammatically incorrect phrase, “We Free Shipping Worldwide,” likely indicating a non-native English speaker administered the site.

Graphics 19 and 20: Google result for sikags[.]com as of 19 May (top) and the front page of the actual site (bottom).27

27https://www.sikags[.]com/
Product Image Theft

Now-defunct fake online shops including jokeapptoday[,]com and vokyn[,]com had email address support@customerservicemobi[,]com listed as additional contact information alongside

https://loungespin[,]com/pages/Contact-Us
On 21 January 2023, a Twitter user indicated that site vroxecom — which also claimed email address support@customerservicemobi.com — had stolen an image of their shop’s necklace. This likely indicates that the creation of these online stores involves taking images from official big brand and independent shops to increase their appearance of legitimacy and display a wide range of products.

Graphics 23 and 24: Tweet from 21 January 2023 claiming image theft by a fraudulent online store.  

Graphic 25: Archived capture of vroxecom’s contact information from 24 January 2023.
Sending Incorrect Merchandise

In the majority of cases, victims did not receive any items following purchases made on these sites and did not receive assistance or replies following attempts to contact the sites. In some cases, victims received hats, scarves, or cheap wallets in place of their ordered item.

![Graphic 26: Scamwatcher reviews for crwarehouse[.com, associated with email address jmservicefor@gmail[.com, show how customers received alternate items or nothing at all following their purchases.]

China Connection

In addition to the templates for these sites tracing back to the Chinese-language shop building tools, these fraudulent online stores provided multiple indications of their Chinese connections and origin. Some of the email addresses identified within the scope of our network — meaning those associated with the Chinese template sites — were also possibly associated with larger scam networks. The following sections detail identifiers related to sites within the scam network.
Shoesdiscounting.favorablebxs[.]com

Fraudulent online store shoesdiscounting.favorablebxs[.]com is associated with Chinese-language template site staticsoe[.]com. As of May and June 2023, the site posed as an official On Running brand site. Three email addresses were associated with the site between at least March and early June 2023, visible on its contact page and in its page source.

Graphics 27 and 28: Overview of shoesdiscounting.favorablebxs[.]com (top) and its association with staticsoe[.]com (bottom), as of 9 June 2023.
Fictional Address

Throughout our investigation, we identified many stores claiming unassociated or imposter locations as their physical address. Website shoesdiscounting.favorablebxs[.]com employed the scam network’s tactic of claiming fictional locations as addresses. The site listed only “Jackson Street, Spring Hill, Kansas 66083” on its contact page between at least March and early June 2023. However, the site’s Terms of Service page provided the full address as 22670 South Jackson Street, Spring Hill, Kansas 66083. The cul-de-sac at this address contains a 22661 and 22671 house number, but no 22670.

40https://shoesdiscounting.favorablebxs[.]com/pages/contact-us
41view-source:https://shoesdiscounting.favorablebxs[.]com/pages/contact-us
42https://shoesdiscounting.favorablebxs[.]com/pages/Terms-of-service_94175af6
43https://shoesdiscounting.favorablebxs[.]com/pages/Terms-of-service_94175af6
usdiscountsing[.]com
The Terms of Service page for shoesdiscounting.favorablebxs[.]com claims the site is operated by usdiscountsing[.]com. Website usdiscountsing[.]com was also associated with Chinese-language template site staticsoe[.]com. As of 13 April 2023, usdiscountsing[.]com was a Chinese-language advertisement for stock market experts. Website usdiscountsing[.]com was likely only active in this format for three to six weeks between mid-March and mid-May, as archived captures of the site from 7 March show it needing additional configuration, and captures from 17 May show the site's content having been removed.

45https://shoesdiscounting.favorablebxs[.]com/pages/Terms-of-service_94175af6
46https://shoesdiscounting.favorablebxs[.]com/pages/Terms-of-service_94175af6
OVERVIEW

This website is operated by usdiscountsing.com. Throughout the site, the terms “we”, “us” and “our” refer to usdiscountsing.com. usdiscountsing.com offers this website, including all information, tools and Services available from this site to you, the user, conditioned upon your acceptance of all terms, conditions, policies and notices stated here.

Graphic 33: Website shoesdiscounting.favorablebxs[.]com identifying its operation by usdiscountsing[.]com.

Graphic 34 and 35: Original Chinese heading (left) and translated English version (right) for usdiscountsing[.]com as of 13 April 2023.

Graphic 36: Site display for usdiscountsing[.]com from between 26 February to 7 March 2023, demonstrating its content advertising stock services was created following that time.
Scam Sites for Sale on Chinese Platforms

Many of the sites involved in the scam were domain names that had been inactive for multiple years and were likely either purchased or stolen and repurposed into new sites. While some of these acquisitions may happen through official domain purchases, some sites may be acquired through indirect means in order to mask their users.

Fraudulent online store vokyn[.]com was identified as for sale on the Chinese-language Q&A forum V2EX on 1 March 2019. V2EX claims to be an online community of start-ups, designers, and developers, where users can post and answer questions related to various technical, creative, trading, and other topics. It is unclear if the domains listed were created by an individual to sell on the forum or if the domain names were hacked or stolen from active sites and resold.

Graphic 37: Domain name vokyn[.]com listed as a domain name for sale on Chinese forum v2ex[.]com as of 1 March 2019.

Graphic 38: Example of vokyn[.]com as associated with the scam network in March 2023. As of May, the site was no longer active.

https://www.crunchbase[.]com/organization/v2ex#:~:text=V2EX%20is%20a%20community%20of,www.v2ex.com
https://tracxn[.]com/d/companies/v2ex/_b1Pe7c5qfl_NJeizExq1EOh5JGJGGOZWS0Ifdd5Jr0
https://www.v2ex[.]com/t/539907
https://www.vokyn[.]com/?path=page/contact

© Nisos - The Managed Intelligence Company® | eCommerce Fraud on the Rise
Chinese Language Site Messages
Fraudulent online stores involved in this scam network are regularly removed. Multiple sites that became inactive provided a Chinese-language message identifying the website was removed by its administrator or indicating that the site could not be found.

Graphics 39 and 40: Original Chinese-language message (top) and English translation (bottom) indicating a site was removed by its administrator.53

53https://www.oofooosale[.]us/
US Connections

Nisos identified a US-based individual who owned multiple fraudulent online stores involved in the scam. We also identified instances of the network posing as official US government representatives.

Postal Service

We identified multiple sites in this network impersonating the United States Postal Service (USPS). This network regularly poses as USPS representatives likely because these sites have a wider potential national audience compared to specialized products and services.

buydiscountusps[.]com

This site claimed to be officially associated with the USPS. It included biographic information, including the name and image for Postmaster General Louis DeJoy and the incorrect image and job description for Chief Information Officer Pritha Mehra on its contact page. The site also included a page citing official USPS COVID-19 policy updates to increase its legitimacy.\(^5\)
Contact Us

We love to hear from you, our team is available to help answer questions and offer styling advice, so if there’s anything you’d like to ask us, we’re right here and ready to help in every way we can.

About [Our Team]

LOUIS DUSOY - Postmaster General

Work to create a long-term, viable operating model for the Postal Service to ensure the organization can fulfill its public service mission.

PRITHA MEHRA - PSC Sales & Services

Provide assistance with products, sales and promotions, and deliver a positive customer experience.

Sort, lift and push moderate to heavy loads of mail and packages to prepare for delivery. Deliver mail along your assigned route. Pick up or collect mail from customers.

Receive customer inquiries, record customer inquiries and complaints, and give customer feedback according to the appropriate process.

PETE GRIFFIN - Transportation Manager

SAPPHIRE - Customer Service Staff

© Nisos - The Managed Intelligence Company® | eCommerce Fraud on the Rise  
Page 28
Contact us

Thanks for your visiting jiangyus.com! If you have any problem, please contact us:

We would love to hear from you, contact us on:

- Email: service@jiangyus.com
- Tel: +1 (865) 471-8342

As of 18 May, the email address for the site was support@discountusps[.]net (top). As of 9 June, the site updated its email address to service@jiangyus[.]com (middle). Email address service@jiangyus[.]com is likely reused from contact information originally created for jiangyus[.]com (bottom).

uspsstamp[.]co

This site claimed its address as 7610 Beverly Blvd, Los Angeles, CA 90048 with email address uspspost.co@outlook[.]com. This address is associated with an actual USPS location. As of 9 June, the site was no longer active. The site was also connected to the staticsoe[.]com template.

Graphics 47 - 49: As of 18 May, the email address for the site was support@discountusps[.]net (top). As of 9 June, the site updated its email address to service@jiangyus[.]com (middle). Email address service@jiangyus[.]com is likely reused from contact information originally created for jiangyus[.]com (bottom).

Graphics 50 and 51: Information listed on the contact page for uspsstamp[.]co, as of 18 May 2023.
Other Sites

We identified many other USPS imposter sites within this network. Some claimed official USPS locations as their addresses, while others claimed likely random residential addresses. Sites like aboutusps[.]shop and uspsdiscount[.]com appeared to sell mattresses and home furnishings as of an 11 June 2023 review, indicating that these sites are likely regularly updated and could quickly be repurposed to or from a USPS imposter site.

Graphics 52 and 53: Overview of aboutusps[.]shop (top) and uspsdiscount[.]com (bottom), as of 11 June 2023. 

https://www.uspsdiscount[.]com/

https://aboutusps[.]shop/

© Nisos - The Managed Intelligence Company® | eCommerce Fraud on the Rise
Conclusion

Scam sites cost financial institutions significant resources and reputational harm when customers are victims of fraud. By putting the pressure and cost on financial institutions to provide reparations, scammers are able to continually prey on victims and expand their reach. Similarly, companies and brands are at risk of financial and reputational harm while criminals target victims using their name. However, the widespread nature of tactics implemented by this scamming network — as well as similar techniques used by other scams — provides avenues whereby diligent investigation can identify indicators of fraud.

Investigators can use the examples listed throughout this report as indicators of potential fraud when considering their own unique situations. In addition to the examples provided above, Nisos researchers support our clients’ unique needs through investigative support and by sharing with investigative teams its pre-existing understanding of existing chargeback threat actors. To help mitigate further fraud and abuse perpetrated by this scamming network and others, Nisos researchers can also provide training to investigators and arbitrators who handle chargeback disputes regarding fraud indicators and how to research pieces of information that are most likely to reveal a hoax. Nisos can help support financial institutions’ efforts to pass this awareness on to their customer base to avoid future fraud. Additionally, when appropriate and upon the direction of its clients, Nisos works closely with local and federal law enforcement agencies to facilitate action against threat actors and e-criminals to unlock capabilities and remedies beyond those of an internal business unit.
Appendix A: Scam Site Format Examples

The following examples demonstrate common features seen across the fraudulent online stores.

Graphics 54 - 56: Examples of a scam site with a top banner and empty contact information page (top), a sale pop-up icon in the bottom-left corner (left), and the SHOP INC copyright (right).

https://logskyer.top/pages/Contact-Us

© Nisos - The Managed Intelligence Company® | eCommerce Fraud on the Rise
Page 32
Appendix B: Scam Site Email Addresses

The following email addresses were identified on scam sites. We do not consider this list to be comprehensive but provide it as an example of the repetitive nature and repurposing of contact information across scam sites.

<table>
<thead>
<tr>
<th>Email</th>
<th>Google Name</th>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jmservicefor@gmail.com">jmservicefor@gmail.com</a>⁶⁹</td>
<td>customer</td>
<td>• Shoesdiscounting.favorablebxs[.]com</td>
</tr>
<tr>
<td></td>
<td>service</td>
<td>• vokyn[.]com</td>
</tr>
<tr>
<td>jerrinelse@gmail[.]com⁷⁰</td>
<td></td>
<td>• shoesdiscounting.favorablebxs[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• geelan[.]shop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ygkrjcpou[.]shop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sb78784[.]shop</td>
</tr>
<tr>
<td>pamelagsgdbell@gmail[.]com⁷¹</td>
<td>Kelly</td>
<td>• asdjh[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• xhfadacaif[.]com</td>
</tr>
<tr>
<td>babybo6355@gmail[.]com⁷²</td>
<td>jianbo</td>
<td>• luluhome[.]shop</td>
</tr>
<tr>
<td></td>
<td>lin</td>
<td>• skechersplus[.]shop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• stahot[.]shop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• birkenstores[.]shop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• lbhot[.]shop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• grillproducts[.]shop</td>
</tr>
<tr>
<td>sarkilsat49@gmail[.]com⁷³</td>
<td></td>
<td>• asdjh[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• bmm-shopify[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• xr-[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cb-shopify[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• bcashley[.]com</td>
</tr>
<tr>
<td>liudang67qq@gmail[.]com⁷⁴</td>
<td></td>
<td>• lasdirectsales[.]shop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• nciwe[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• werfew[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• wsaze[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• dreamtoning[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• kicksmalls[.]com</td>
</tr>
<tr>
<td>boatengstephen571@gmail[.]com⁷⁵</td>
<td>Stephen Boa</td>
<td>• qoobmm[.]site</td>
</tr>
<tr>
<td>usdiscountsing@gmail[.]com⁷⁶</td>
<td></td>
<td>• shoesdiscounting.favorablebxs[.]com</td>
</tr>
<tr>
<td>support@customerservicemobi[.]com⁷⁷</td>
<td></td>
<td>• jokeapptoday[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• vokyn[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• vroxel[.]com</td>
</tr>
<tr>
<td>service@ez-malls[.]ca⁷⁸</td>
<td></td>
<td>• jokeapptoday[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sportkicksale[.]com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• evaneich[.]com</td>
</tr>
<tr>
<td>a1127040642@gmail[.]com⁷⁹</td>
<td>jian zhang</td>
<td>• dreamtoning[.]com</td>
</tr>
<tr>
<td>service@flightshape[.]com⁸⁰</td>
<td></td>
<td>• comfortables[.]shop</td>
</tr>
</tbody>
</table>

⁶⁹https://www.vokyn[.]com/?path=page/contact
⁷⁰https://shoesdiscounting.favorablebxs[.]com/pages/contact-us
⁷¹https://xhfadacaif[.]com/pages/Contact-Us
⁷²https://www.bbb[.]org/scamtracker/lookupscam/671125
⁷³https://asdjh[.]com/pages/Contact-Us
⁷⁴https://www.lasdirectsales[.]shop/
⁷⁵view-source:https://qoobmm[.]site/pages/Contact-Us
⁷⁶https://shoesdiscounting.favorablebxs[.]com/pages/Terms-of-service_94175af6
⁷⁷https://www.vokyn[.]com/?path=page/contact
⁷⁸https://www.jokeapptoday[.]com/pages/Contact-Us
⁷⁹view-source:https://www.dreamtoning[.]com/pages/Contact-Us_a494d46b
⁸⁰https://www.comfortables[.]shop/pages/Contact-Us
The following addresses are just a few examples claimed by the many fraudulent online stores. These addresses demonstrate how the online stores claimed: non-existent addresses; locations associated with the brands they impersonated; home addresses for random, unassociated individuals; and random locations.

<table>
<thead>
<tr>
<th>Address</th>
<th>Example Domain</th>
<th>Actual Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>22670 South Jackson Street, Spring Hill, Kansas 66083</td>
<td>shoesdiscounting.favorablebxs.com</td>
<td>Does not exist</td>
</tr>
<tr>
<td>14555 Valley Center Dr, Victorville, CA 92395</td>
<td>birkenstores[,]shop luluhome[,]shop onlineboots[,]shop stahot[,]shop monhouse[,]shop</td>
<td>Costco store</td>
</tr>
<tr>
<td>2747 Wolfcreek Lane Memphis, TN 3811</td>
<td>samashop[,]top</td>
<td>Skechers outlet</td>
</tr>
<tr>
<td>606 North Morgan Street, Shelbyville, Illinois 62565</td>
<td>glorypretty[,]com</td>
<td>Home address for a likely random, unassociated individual</td>
</tr>
<tr>
<td>1225 NW 27th St, Oklahoma City, OK 73106</td>
<td>gasfnl[,]com</td>
<td>Home address for a likely random, unassociated individual</td>
</tr>
<tr>
<td>212 Horton Road, Datchet, Slough, England, SL3 9HL</td>
<td>sheinsshop[,]com</td>
<td>Likely residential address associated with multiple scam businesses and sites^{88,89,90}</td>
</tr>
</tbody>
</table>

---

^{81}https://onlinellb[,]shop/page/custom/contact-us
^{82}https://glorypretty[,]com/faqs/
^{83}https://glorypretty[,]com/refund-policy/
^{84}https://www.bbb[,]org/scamtracker/lookupscam/704734
^{85}https://community.shopify[,]com/c/shopify-discussions/getting-the-credentials-of-a-shopify-store-that-ripped-me-off/td-p/2043374
^{86}https://www.amaps[,]xyz/contact-us.html
^{87}https://shoesdiscounting.favorablebxs[,]com/pages/Terms-of-service_94175af6
^{88}https://www.zoopla[,]uk/property/lsrm/100080369746/
^{89}https://find-and-update.company-information.service.gov[,]uk/company/11934935/filing-history
^{90}https://www.onlinethreatalerts[,]com/article/2023/2/28/is-ressrobe-a-scam-or-legit-online-store-review-of-ressrobe-com/
Graphic 57: Example of fraudulent online store sheinsshop[.]com claiming an address in Slough, England and specifying it as not a return address, likely because the scammers were not actually associated with the address. 91

The scam sites regularly displayed previous email addresses through their page source. Many sites that previously had email addresses have also completely removed all forms of contact information from the pages, limiting victims’ potential to interact with the company.

Graphic 58 and 59: Example of xhfadacai[.]com containing two email addresses on its contact page (top) and a previous address in its page source (bottom), as of 28 April 2023. 92 93

91 https://sheinsshop[.]com/page/custom/contact-us
92 https://xhfadacai[.]com/pages/Contact-Us
93 view-source:https://xhfadacai[.]com/pages/Contact-Us
La Sportiva

Please feel free to contact us if you have any problem.

jmservicefor@gmail.com
Customer service hours: Monday to Saturday
Us time: 21:00–6:00
Australian time: 11:00–20:00
UK time: 2:00–11:00

La Sportiva

Please feel free to contact us if you have any problem.

liudang67qq@gmail.com
Customer service hours: Monday to Saturday
Us time: 21:00–6:00
Australian time: 11:00–20:00
UK time: 2:00–11:00

La Sportiva

Please feel free to contact us if you have any problem.

Customer service hours: Monday to Saturday
Us time: 21:00–6:00
Australian time: 11:00–20:00
UK time: 2:00–11:00

Graphics 60 - 62: Example of lasdirectsales.com having email address jmservicefor@gmail.com as early March 2023 (top) and email address liudang67qq@gmail.com as of 28 April 2023 (middle). As of 9 June, the site did not list any email address on its contact page (bottom).
Appendix C: Company Names on Bank Statements

We provide the following additional information on company names identified on victims' bank statements following their purchases from fraudulent online stores. These examples are likely associated with China-based or China-adjacent actors.

AP buygoodsing Singapore

A victim of crwarehouse[/.]com — associated with email address jmservicefor@gmail[/.]com — and a victim of hangwag.com[/.]se both claimed that their credit card statements included “AP buygoodsing SINGAPORE” or “AP *buygoodsing SINGAPORE” following purchases from the fraudulent sites. Hanwag[/.]com.se used variations of email addresses including auto6@vmcustomers[/.]com and auto4@vmcustomers[/.]com.95
Graphics 63 and 64: Examples of AP buygoodsing Singapore and variations of vmcustomer[.]com email addresses used on other fraudulent sites.⁹⁶ ⁹⁷

It is possible that AP buygoodsing SINGAPORE is associated with buygoodsing[.]com, a website that has been identified on scam monitoring websites and customer reviews as fraudulent.⁹⁸ ⁹⁹ Many of the scam reports from victims claim they ordered shoes or other items and instead received a cheap wallet.¹⁰⁰
Although this store is allegedly associated with and located in Singapore, the site used a China-located service Cloud Yuqu LLC through diymysite[.]com for its registration.\footnote{https://es.scamdoc[.]com/whois?id=1110243#registrant} \footnote{https://www.trustpilot[.]com/review/buygoodsing[.]com} \footnote{https://myip[.]ms/view/web_hosting/1017160/Cloud_Yuqu_Llc.html} As of early June 2023, the site has also been associated with a Hong Kong-based IP address since at least October 2022.

Graphic 65: Sample of many reviews from late 2022 and early 2023 identifying buygoodsing[.]com as a scam.\footnote{https://myip[.]ms/view/web_hosting/1017160/Cloud_Yuqu_Llc.html}
**Graphic 66:** Contact information for buygoodsing[.]com, listed on its official website between at least March and early June 2023.104

**Graphic 67:** Registration information for buygoodsing[.]com indicating Cloud Yuqu LLC.105

**Helipay Lovetheshops**

A victim of oroton-bags[.]shop — associated with email address jmservicefor@gmail[.]com — and a victim of it-stradivarius[.]shop identified “Helipay Lovetheshops” or “Helipay*lovetheshops” on their credit statements. Similar to other sites, customers reported either not receiving any merchandise or receiving a scarf when they had ordered furniture or musical instruments.106 107

104https://buygoodsing[.]com/
105https://es.scamdoc[.]com/whois?id=1110243#registrant
106https://www.yourlifeupdated[.]net/web/attenzione-alle-mail-da-johnmgray2322gmail-com-truffa/
107https://www.yourlifeupdated[.]net/web/attenzione-alle-mail-da-service822cplay-com-truffa/

© Nisos - The Managed Intelligence Company® | eCommerce Fraud on the Rise

Page 40
Some victims also identified the merchant name appearing as or including a variation of “shen zhen shi CN,” which likely refers to the city of Shenzhen, China. Contact between a customer who received the wrong item in late January 2023 and a representative from Helipay Lovetheshops requested multiple iterations of “confirmation” information to prove that the customer did not receive the correct item. Its final response from 8 February 2023 — following the customer asking for their money back and not for a new package — requested the customer to send their payment number. No information was available regarding the victim’s success in receiving a refund; however, a resolution seems unlikely.

![Comments from those who bought from johnmgray2322@gmail.com](image)

**Graphic 68: Reviews from Italian-language site identifying “helipay *lovetheshops shen zhen shi CN” associated with email address johnmgray2322@gmail.com.” Translated from Italian.**

---

108https://www.yourlifeupdated.net/web/attenzione-alle-mail-da-johnmgray2322gmail-com-truffa/

© Nisos - The Managed Intelligence Company® | eCommerce Fraud on the Rise

Page 41
Portions of an interaction between a customer who received the wrong item and customer support, with the final message on 8 February.¹⁰⁹