Examining Security Risks in Logistics APIs Used by Online Shopping Platforms

Ryan Flores, Charles Perine, Lord Remorin, Roel Reyes

TREND MICRO | research

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

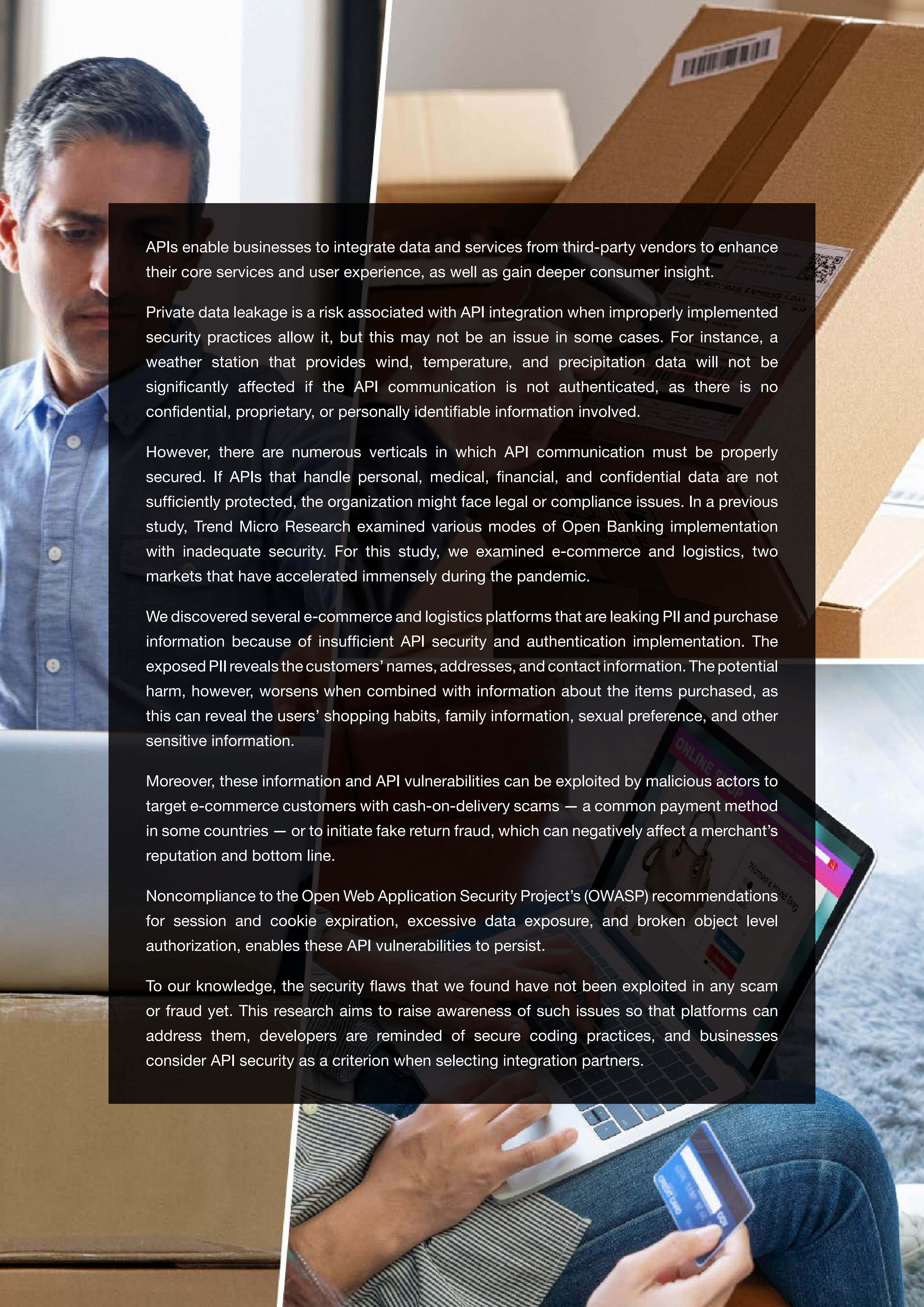
Published by
Trend Micro Research

Written by
Ryan Flores,
Charles Perine,
Lord Remorin,
Roel Reyes,
Trend Micro Research

Stock images used under license from
Shutterstock.com

For Raimund Genes (1963-2017)

Contents



APIs enable businesses to integrate data and services from third-party vendors to enhance their core services and user experience, as well as gain deeper consumer insight.

Private data leakage is a risk associated with API integration when improperly implemented security practices allow it, but this may not be an issue in some cases. For instance, a weather station that provides wind, temperature, and precipitation data will not be significantly affected if the API communication is not authenticated, as there is no confidential, proprietary, or personally identifiable information involved.

However, there are numerous verticals in which API communication must be properly secured. If APIs that handle personal, medical, financial, and confidential data are not sufficiently protected, the organization might face legal or compliance issues. In a previous study, Trend Micro Research examined various modes of Open Banking implementation with inadequate security. For this study, we examined e-commerce and logistics, two markets that have accelerated immensely during the pandemic.

We discovered several e-commerce and logistics platforms that are leaking PII and purchase information because of insufficient API security and authentication implementation. The exposed PII reveals the customers' names, addresses, and contact information. The potential harm, however, worsens when combined with information about the items purchased, as this can reveal the users' shopping habits, family information, sexual preference, and other sensitive information.

Moreover, these information and API vulnerabilities can be exploited by malicious actors to target e-commerce customers with cash-on-delivery scams — a common payment method in some countries — or to initiate fake return fraud, which can negatively affect a merchant's reputation and bottom line.

Noncompliance to the Open Web Application Security Project's (OWASP) recommendations for session and cookie expiration, excessive data exposure, and broken object level authorization, enables these API vulnerabilities to persist.

To our knowledge, the security flaws that we found have not been exploited in any scam or fraud yet. This research aims to raise awareness of such issues so that platforms can address them, developers are reminded of secure coding practices, and businesses consider API security as a criterion when selecting integration partners.

Introduction

In 2020, 131 billion parcels were shipped worldwide,[1] a significant number of which was driven by the growth of e-commerce[2] at a time when lockdowns were enforced to curb the spread of the pandemic. People still needed to shop while retailers still needed to sell goods, but with movement restrictions in place as well as health and safety concerns, e-commerce provided the platform for businesses to continue selling to their customers.

Aside from the platforms used to sell and pay for merchandise, fulfillment services play a big part in e-commerce. Without these services, consumers won't be able to receive the packages they bought online. However, only the biggest retailers like Amazon can set up their own logistics service, so most merchants need to integrate with a logistics provider to ship their products to their customers.

Logistics providers offer a seamless experience, such as order and tracking notifications that are made to look like they are coming from the merchants even if the updates are being sent by the external logistics providers. To do this, e-commerce platforms integrate with logistics systems platforms like third-party logistics (3PL) to pass along shipping information. This creates a situation in which a security weakness in the application programming interface (API) or authentication chain can disclose customers' personally identifiable information (PII) through HTTP replay attacks because of weak or inadequate means of authentication.

This research paper examines the security flaws that we have seen in the API implementation of logistics providers that can potentially leak PII. We explore the various implications and security risks these flaws present to merchants and buyers alike.

Background

Even before the pandemic happened, e-commerce was already gaining momentum and growing at the rate of 4.5% per year globally.[3] The pandemic lockdowns merely accelerated the adoption of e-commerce because it significantly reduced person-to-person interaction to address the safety concerns during the pandemic.

Compared to a physical store, e-commerce has several advantages:

- **Lower initial capital.** One of the most capital-intensive components of retail is having a physical store, aside from a warehouse. E-commerce removes the need for an actual physical store and a warehouse, thus reducing the start-up cost.
- **Open 24/7.** Buyers can shop in online stores round-the-clock and are not bound by store or mall hours.
- **Wider reach.** E-commerce enables merchants to engage customers that are hundreds or even thousands of miles away.

It must be pointed out that setting up an e-commerce business requires a more cyber-savvy background compared to building a physical store. To illustrate the scenario, let us use a fictitious retailer named XYZ Store that wants to put up an e-commerce store to complement its physical store.

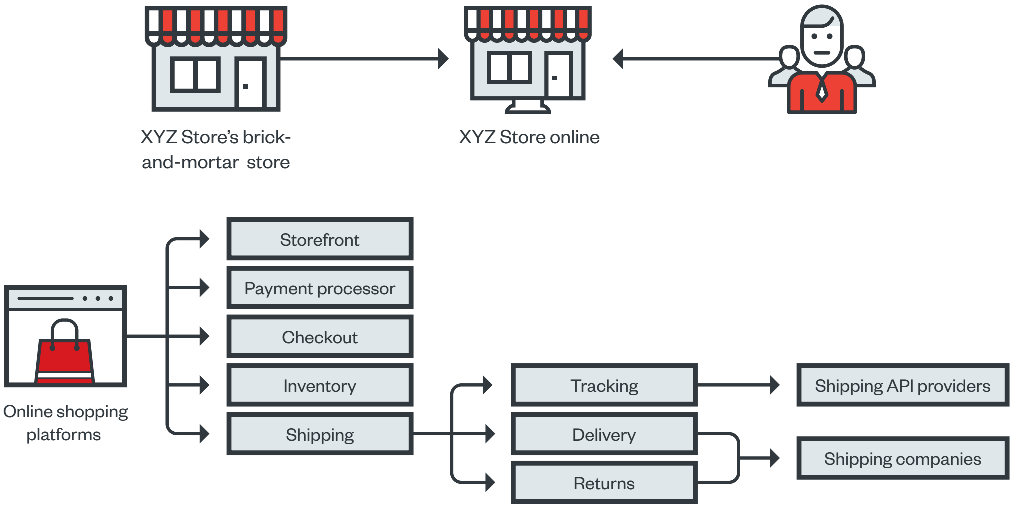


Figure 1. Requirements for establishing an online store

First, XYZ Store needs to have a storefront or a place on the internet where it can showcase the items it is selling. The storefront can be XYZ Store's own website, which gives it complete freedom to design the look and feel of the website, as well as control the branding and customer experience. However, operating its own website comes with other responsibilities, such as website development, domain registration, and website hosting and maintenance.

XYZ Store then needs to have a way for customers to pay for their purchases and a way for the store to receive payment. To do this, it needs to incorporate a payment gateway into the storefront to process payments.

Lastly, XYZ Store needs a logistics provider that can ship the merchandise to its customers and provide order tracking information. Many logistics providers categorized as third-party logistics (3PL) or fourth-party logistics (4PL) handle not only parcel delivery, but also inventory, warehousing, and order tracking.

Note that some platforms, such as Amazon,[4] eBay,[5] Shopify,[6] and Lazada,[7] offer all-in-one solutions so that merchants only need to register with their platform. The setup of the storefront, payment gateway, and logistics is just a matter of ticking off checkboxes, thus making it very convenient for businesses new to e-commerce. Of course, the trade-off to this convenience offered by such platforms is the lack of options, so much so that storefronts look so similar to those of other merchants, or the vendor options for payment gateways and logistics might be limited to those already integrated to the platform. For the less cyber-savvy retailers, the appeal of e-commerce platforms is the low bar of technical knowledge needed to build an online store.

There are still some areas where a physical store has advantages over online stores, such as the following:

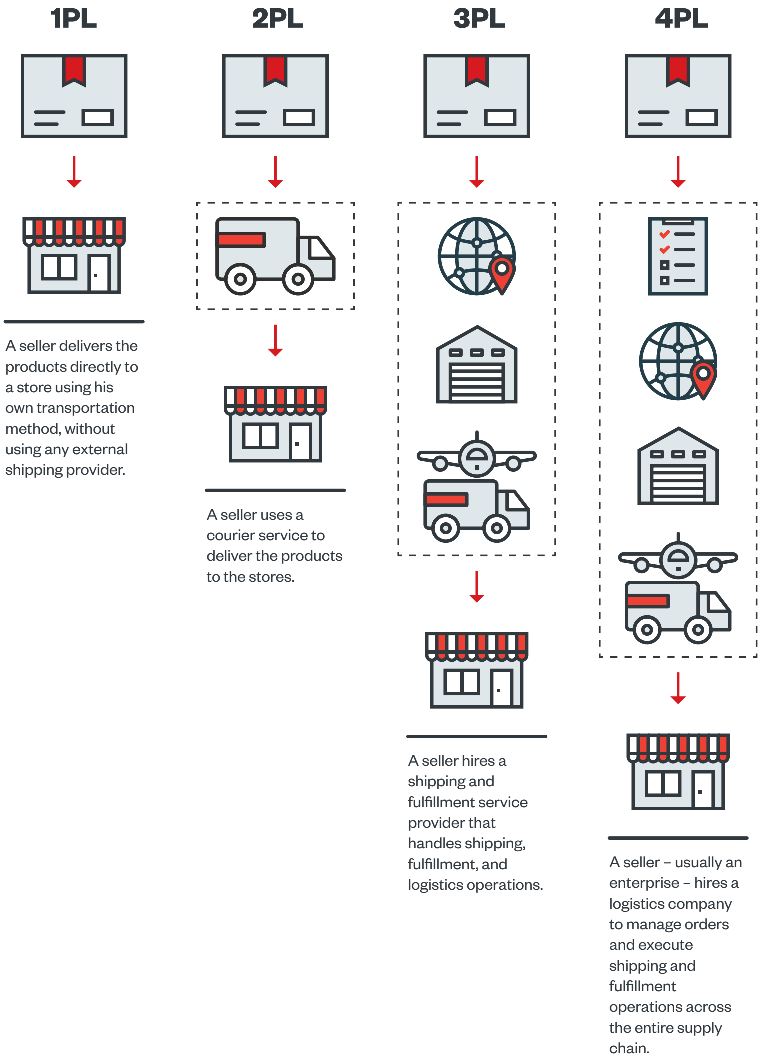
- **Customers can see, inspect, and test items.** The potential buyer can see and hold the product, try it on, test it, check how it really feels and looks while they are in the physical store.
- **Customers can take the product home right after purchase.** Customers just need to pay for the item and they can immediately take it with them.
- **No shipping cost**. Although a lot of e-commerce platforms offer free or reduced shipping fees, expedited shipping and the shipping of fragile items can be costly.
- **Simple return process.** Since the purchase is made in person, the return process can also be made in person and is less complicated compared to an online transaction. The customer does not need to trigger the return process, print labels, and wait for the courier to pick-up the parcel or drop off the item for return at the post office.

The advantages of the physical store are gaps that e-commerce platforms, logistics providers, and emerging technologies are trying to bridge. The use of high-quality photos, 3D models, videos, customer reviews, unboxing experiences, and virtual reality all try to narrow the gap between merely seeing the item on the screen and having a more immersive shopping experience, which helps compensate for some of the shortfalls of not being able to physically handle the product.

Logistics platforms are working vigorously to offer faster turnaround times in their deliveries, with next-day deliveries becoming more common while same-day deliveries are being rolled out in some locations. This quick turnaround enables e-commerce platforms to minimize the gap between the customers walking away from the physical store with the item in hand, and the customers receiving the package a few hours after they placed their order online.

What are External Logistics Providers?

As consumer demand shifts to e-commerce, business owners need to keep up with fulfilling orders to prevent delays in product delivery. To help ease the merchants' logistical tasks, an external logistics provider is a viable option for managing the supply chain logistics process, either partially or through a complete logistics solution. This can be a simple courier service that merchants use to deliver products (2PL) or a 3PL that manages warehousing, fulfillment, and delivery of products. Figure 2 shows how an external logistics provider works for different use cases.[8]



A seller delivers the products directly to a store using his own transportation method, without using any external shipping provider.

A seller uses a courier service to deliver the products to the stores.

A seller hires a shipping and fulfillment service provider that handles shipping, fulfillment, and logistics operations.

A seller – usually an enterprise – hires a logistics company to manage orders and execute shipping and fulfillment operations across the entire supply chain.

Figure 2. How an external logistics provider functions for different use cases

For a new business, an account with a courier provider is required to deliver products to its customers. Eventually, when demand increases and the online store becomes popular, the store owner needs to find other external logistics providers to keep up with the orders, whether for warehousing, fulfillment, or delivery of goods. E-commerce platforms are a good solution for store owners to easily manage their online business with a minimal learning curve and ease in setting up web servers and domain names.

E-commerce platforms allow merchants to choose add-on services or external logistics providers depending on the requirements of the business. For example, merchants using an e-commerce platform can have a subscription account that manages the delivery of their products and have a separate account from another provider that manages warehousing. E-commerce platforms can also manage 3PL providers which makes them a 4PL.

In addition, during the pandemic, the dropshipping business became more popular because it is easy to set up and does not use any warehousing to store bulk inventories from a manufacturer. As shown on Figure 3,[9] dropshipping allows merchants to order directly from suppliers on the customers' behalf, so that products are shipped directly to them without the need for a warehouse to store the goods. E-commerce platforms act as external logistics providers by enabling integrations to allow the direct purchase from suppliers and send them straight to the consumers.

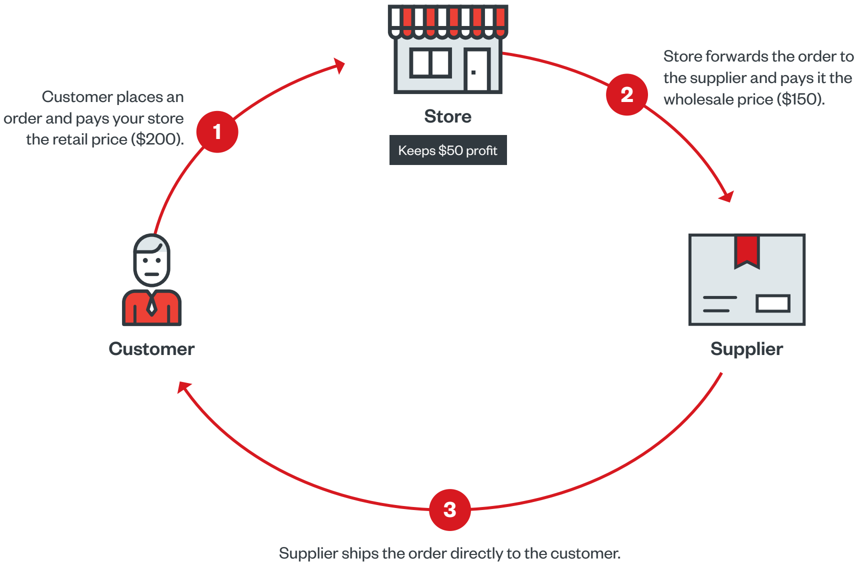

Store
Keeps $50 profit
Customer places an order and pays your store the retail price ($200).
1
Store forwards the order to the supplier and pays it the wholesale price ($150).
2
Customer
Supplier
3
Supplier ships the order directly to the customer.

Figure 3. How the dropship model works

During this research, we initially looked at 3PL and 4PL providers that were inadvertently leaking consumers' personal information through unauthenticated or unsecure methods. We also identified that it is not only 3PL and 4PL platforms that can expose sensitive information but also services that are integrated with them. E-commerce platforms allow merchants to integrate existing external logistics providers through APIs to seamlessly consolidate different services into a single platform. API keys and authentication keys are registered so an e-commerce platform and external logistics providers can communicate securely.

PII Leakage From E-Commerce Platforms and Third-Party Logistics Providers

Every e-commerce platform has its own way of securing customers' order information. The most common method is to require customers to log in to an account before viewing the details of an order. However, due to the convenience of using the guest checkout option on marketplaces, logging in with an account is just one of the options to view the online order information. Another option is to use unique URLs that e-commerce platforms send to the customers by email or SMS that redirects them to a website where the order information can be found. This allows guest users to check the status of their purchases without needing to authenticate the session. This approach presumes that the combination of using a unique URL sent to an email address or phone number owned by the recipient sufficiently ensures the protection of PII.

Unfortunately, this situation creates a false sense of security for operators of e-commerce platforms who assume that anyone who visits the URL with the corresponding URL parameters is the legitimate customer who made the purchase. Despite the use of Secure Sockets Layer (SSL) to guarantee an encrypted connection between the client and the server, the URL links to access the order information can still be retrieved in the following situations:

- The URLs can be logged by a web server for debugging or for tracking web traffic.
- The URLs accessed by the consumers may appear on their browsing history.
- The URLs have been collected by the consumers' browser extension.
- The URLs are visible to network administrators performing SSL interception using trusted certificates.
- The URLs appear in router logs or proxy logs.
- The URLS are captured through the interception of rogue Virtual Private Network (VPN) service operators.
- The SMS sent by e-commerce platforms containing the tracking information links are intercepted by malicious actors.

- The URLs are visible in security and employee monitoring products.
- The URLs are collected through external web trackers.[10]
- The URLs are collected in bug reporting software being implemented in various applications.
- The URLs are retrieved through third-party tracking domains that intercept form data.[11]

Notably, the problem of leaking PII from URL query parameters is not exclusive to e-commerce platforms and logistics APIs but has also been seen multiple times on different verticals as extensively discussed in a report we published about open banking APIs[12] and the airline industry as well.[13] In the open banking and airline API information leaks, so-called "telltale" information can be found in the URLs, but this is different from what we found in the traffic of e-commerce platforms and logistics API as those did not contain PII or telltale information in the URLs. Rather, reusing the tracking URL can reveal information that should be visible only to the users.

Directly accessing a URL without further authentication is not the only way to retrieve a customer's PII. Communication between external logistics providers using API to provide seamless integration can lead to PII exposure. This can happen if the tracking link visited by a user needs to make a query through an external service provider to get data and render the information for customers to view. We observed this flaw in the 3PL API services that we were investigating, which will be explained further in the next section.

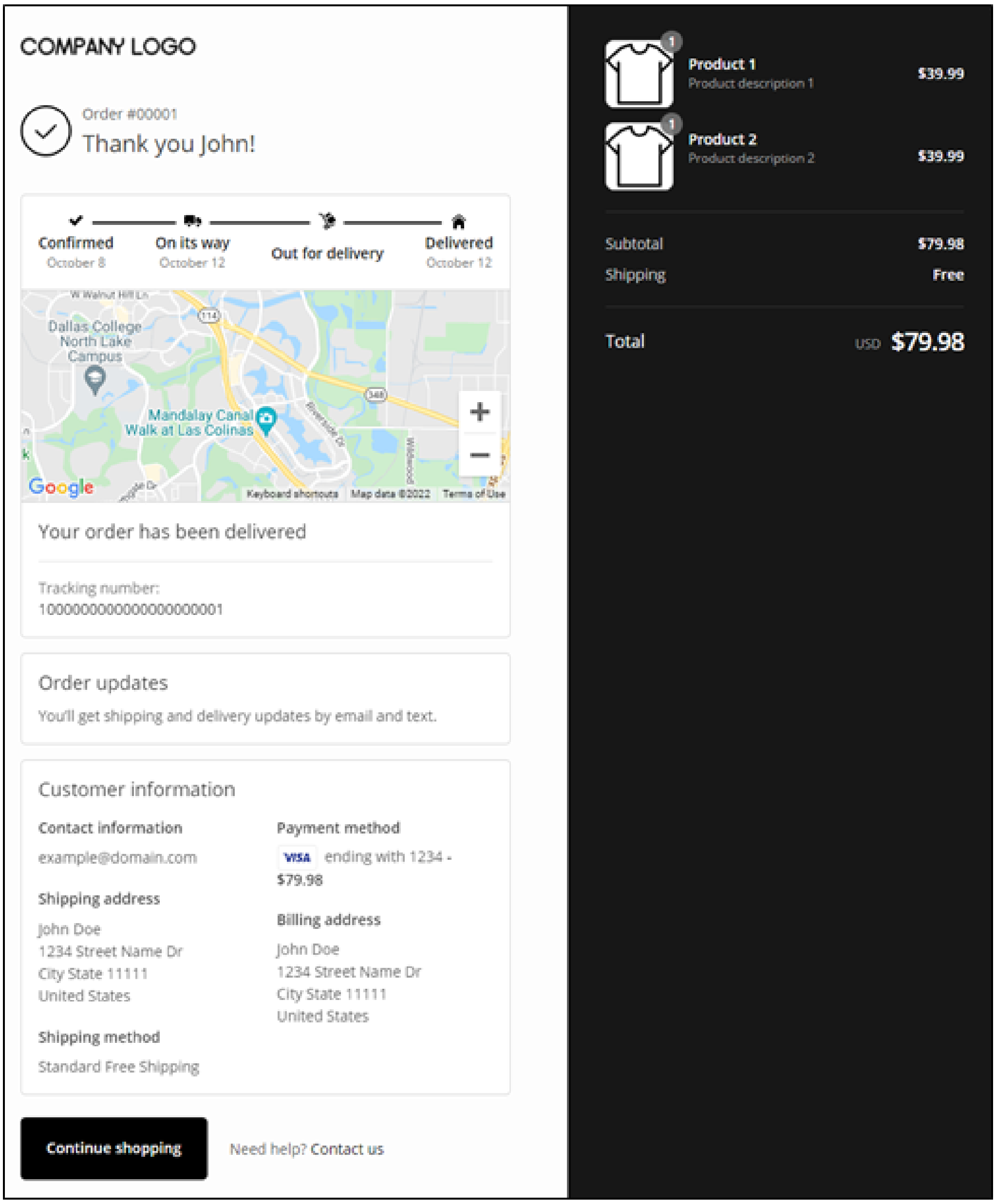
Bear in mind that even though PII is not disclosed in URL parameters, failure to implement authentication or verification of session cookies when visiting or redirecting to a URL is still risky when protecting the customers' PII since anyone who has information about the URL path can visit it and retrieve customer data. The following section elaborates the various flaws that we found in 3PL services and an e-commerce platform that leak customers' PII through unauthenticated methods.

Authentication Keys in URL Parameters

During our research, we looked at many different online stores and found that the security for each online store and e-commerce platform varies. What's interesting about our findings is that some online stores are displaying our order information — including PII — without requiring us to log in to their website. We found that these online stores are hosted in an e-commerce platform and this flaw is not only limited to several online stores that we ordered from but in all the stores hosted on their platform.

When consumers place an order in an online store, they will receive a confirmation email with a URL link including the authentication key on the URL parameter to view the order details. This key is used to verify if the user checking the order page is the recipient of the email. The order page contains the following information:

- Order status
- Tracking information
- Items purchased, including the price
- Customer name
- Contact information of the buyer (email address and/or phone number)
- Payment method
- Shipping and billing address



COMPANY LOGO

Order #00001

Thank you John!

Confirmed October 8 — On its way October 12 — Out for delivery — Delivered October 12

Your order has been delivered

Tracking number:
1000000000000000000001

Order updates

You'll get shipping and delivery updates by email and text.

Customer information

Contact information
example@domain.com

Shipping address
John Doe
1234 Street Name Dr
City State 11111
United States

Shipping method
Standard Free Shipping

Payment method
VISA ending with 1234 - $79.98

Billing address
John Doe
1234 Street Name Dr
City State 11111
United States

Continue shopping

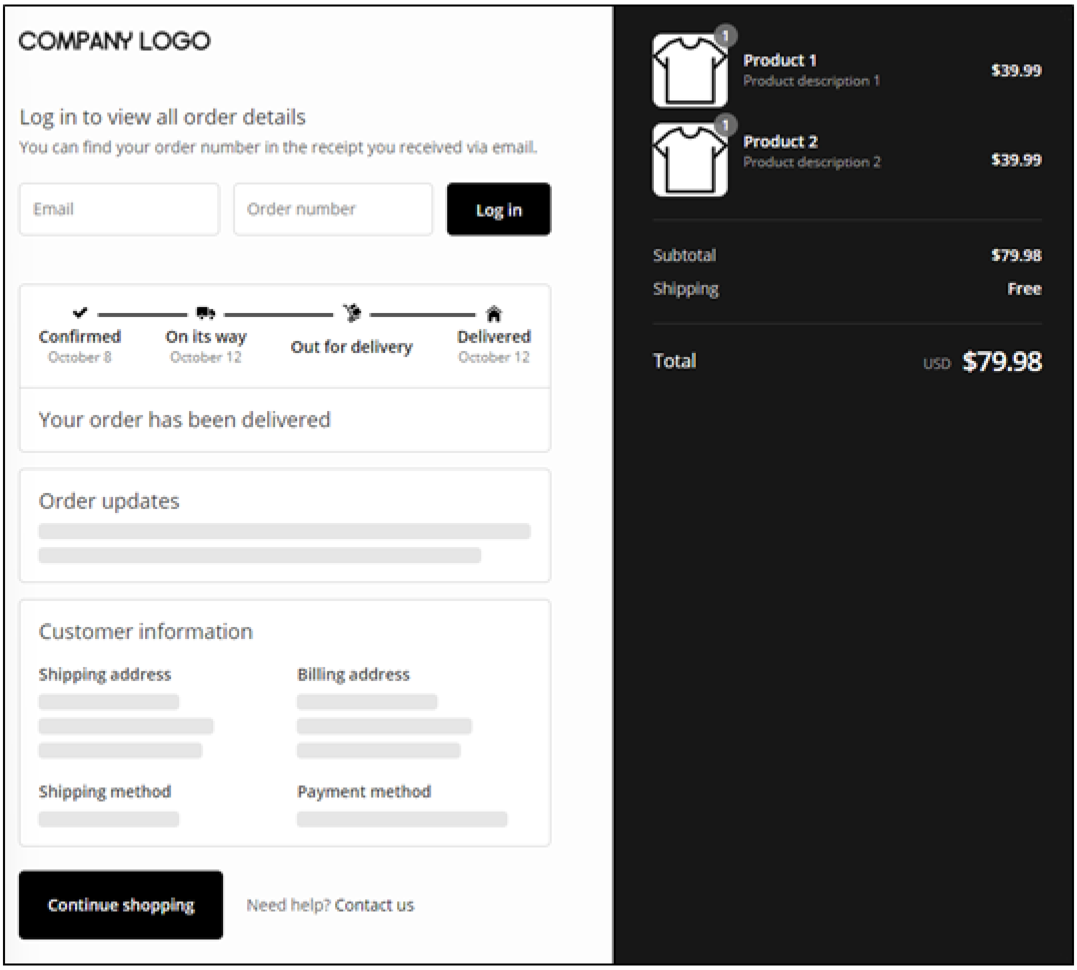
Need help? Contact us

Product 1 Product description 1	1	$39.99
Product 2 Product description 2	1	$39.99

Subtotal	$79.98
Shipping	Free
Total	USD $79.98

Figure 4. The customer's PII is shown despite the lack of proper authentication

If the authentication key is removed from the URL request, the order and tracking page still loads, but the customer's PII is automatically redacted, which should be the correct way to display order information without authentication.



COMPANY LOGO

Log in to view all order details

You can find your order number in the receipt you received via email.

Your order has been delivered

Order updates

Customer information

Need help? Contact us

Product 1 — Product description 1 — $39.99

Product 2 — Product description 2 — $39.99

Subtotal $79.98

Shipping Free

Total USD $79.98

Figure 5. The customer's information is redacted when the authentication key on the URL query string is removed.

Passing authentication keys as part of the URL parameter is an unsafe method of securing a customer's PII since authentication keys can still be retrieved in various ways, such as through a customer's browsing history, router logs, among other means. The use of unencrypted URL query parameters has long been a concern as this method makes customers' PII susceptible to sniffing and man-in-the-middle attacks.[14] This same method of authentication via authentication key in the URL is also used for non-guest accounts, which defeats the purpose of securing an account by signing up to an online store.

We also noticed that the URL links to the order information does not expire. We found orders dating back to 2016. We then accessed the order information link and verified that it is still valid and the information about both the order and customer can still be viewed.

PII Leakage Through Unauthenticated 3PL APIs

3PL providers offer services to online retailers for their logistical needs like shipping, tracking, and processing of orders. However, we found a 3PL provider's API (Company X) disclosing customers' PII through an unauthenticated API service. This API service is being used by four other 3PL providers to display customers' order information.

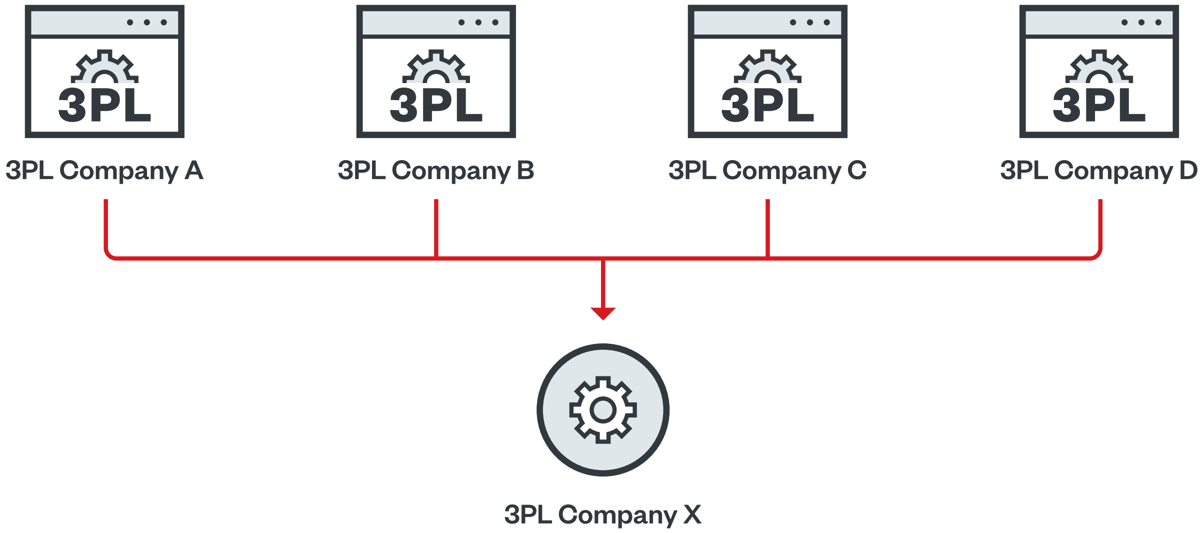
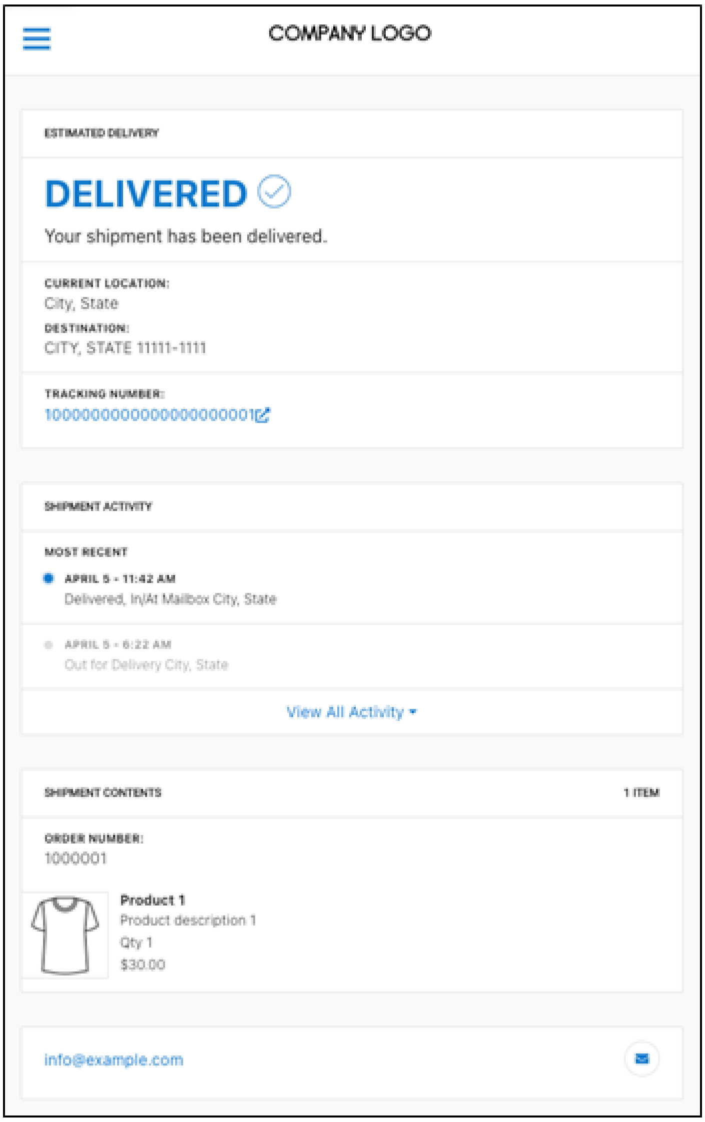


Figure 6. Four 3PL companies using another 3PL company's API to retrieve order and tracking information

While checking on the order information page from the URL link provided by one of the four 3PL providers, we didn't find any sensitive customer information. It only displayed high-level tracking information details, the status of the order, and the items purchased.



COMPANY LOGO

ESTIMATED DELIVERY

DELIVERED ✓

Your shipment has been delivered.

CURRENT LOCATION:
City, State

DESTINATION:
CITY, STATE 11111-1111

TRACKING NUMBER:
1000000000000000000001

SHIPMENT ACTIVITY

MOST RECENT

● APRIL 5 • 11:42 AM
Delivered, In/At Mailbox City, State

● APRIL 5 • 6:22 AM
Out for Delivery City, State

View All Activity ▾

SHIPMENT CONTENTS — 1 ITEM

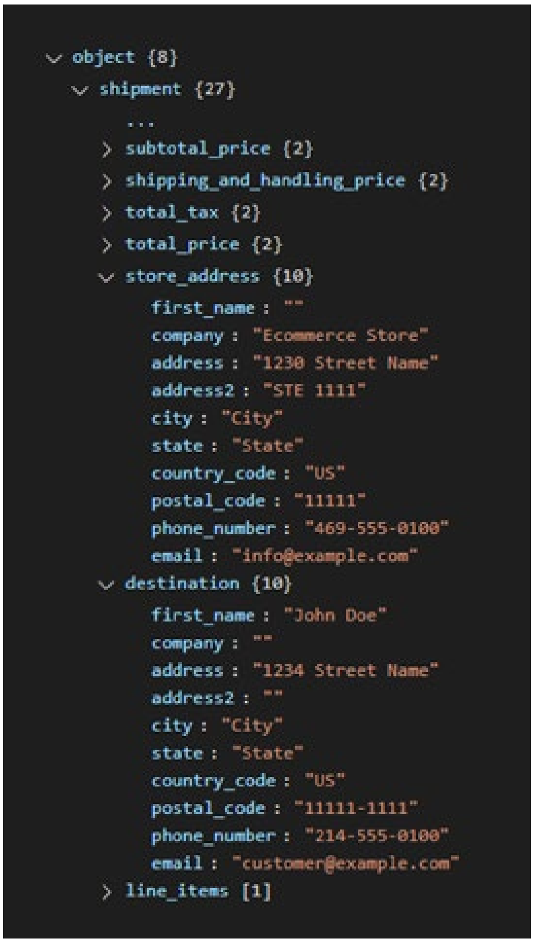
ORDER NUMBER:
1000001

Product 1
Product description 1
Qty 1
$30.00

info@example.com

Figure 7. Order details from a 3PL company that does not display a customer's PII

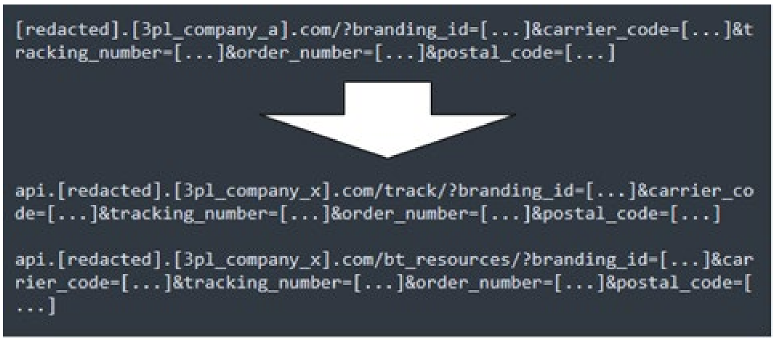
However, when following the HTTP request made to view the order details, we discovered that the page we were viewing was making an HTTP request in the background to another 3PL provider to obtain the order details.



```
∨ object {8}
  ∨ shipment {27}
      ...
    > subtotal_price {2}
    > shipping_and_handling_price {2}
    > total_tax {2}
    > total_price {2}
    ∨ store_address {10}
        first_name : ""
        company : "Ecommerce Store"
        address : "1230 Street Name"
        address2 : "STE 1111"
        city : "City"
        state : "State"
        country_code : "US"
        postal_code : "11111"
        phone_number : "469-555-0100"
        email : "info@example.com"
    ∨ destination {10}
        first_name : "John Doe"
        company : ""
        address : "1234 Street Name"
        address2 : ""
        city : "City"
        state : "State"
        country_code : "US"
        postal_code : "11111-1111"
        phone_number : "214-555-0100"
        email : "customer@example.com"
    > line_items [1]
```

Figure 8. Data retrieved from an API request showing a full set of customer information

Checking the URL parameters of the URL for the order information page and the two API requests made in the background showed that the values passed on the URL parameters were similar. One API request going to the “track” subdirectory returned the high-level tracking information with no PII. However, another API request to the “bt_resource” subdirectory that used an unauthenticated method to verify API requests returned a full set of information about the seller, buyer, and purchased items. Therefore, anyone who has access to the order information URL can reconstruct the URL to retrieve a customer’s PII and order details.



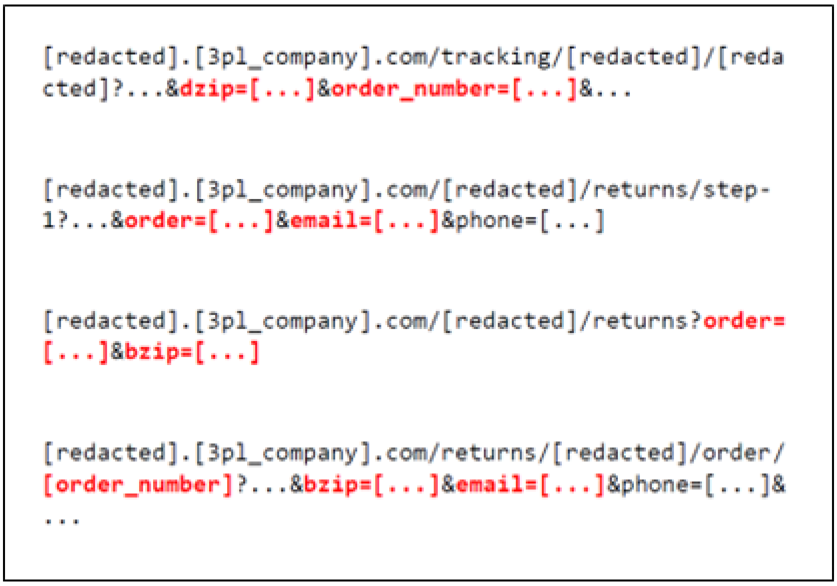
```
[redacted].[3pl_company_a].com/?branding_id=[...]&carrier_code=[...]&t
racking_number=[...]&order_number=[...]&postal_code=[...]

api.[redacted].[3pl_company_x].com/track/?branding_id=[...]&carrier_co
de=[...]&tracking_number=[...]&order_number=[...]&postal_code=[...]

api.[redacted].[3pl_company_x].com/bt_resources/?branding_id=[...]&car
rier_code=[...]&tracking_number=[...]&order_number=[...]&postal_code=[
...]
```

Figure 9. Redirection of URL from one 3PL company to another

Unlike the e-commerce platform mentioned previously, the URL links to view the order information from these 3PL providers had been set to expire after a few months.

Order Identification in URL Parameters

We found another 3PL company indirectly leaking customer PII. Checking an order's information showed that only the high-level tracking information about the order is displayed. Additionally, the items ordered are sometimes shown but not the information about the customer, depending on the online retailer. However, while examining the URL parameters, we found pieces of information that can be used to retrieve the PII of customers, such as the order number, destination ZIP code, and email address.

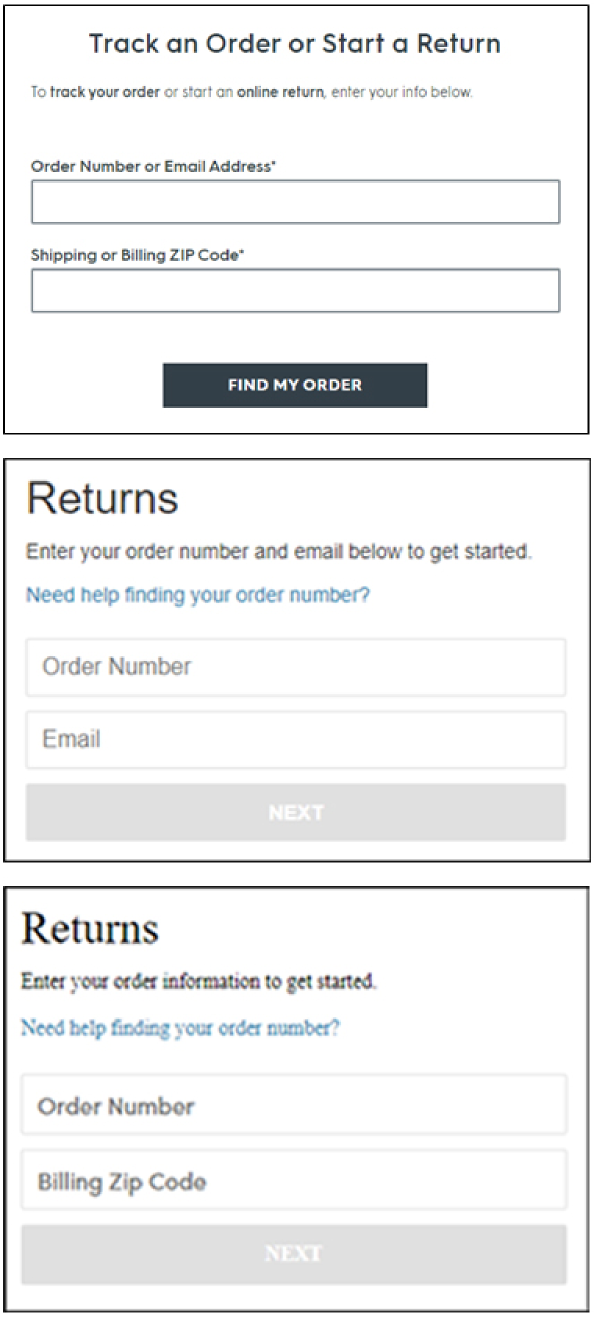


```
[redacted].[3pl_company].com/tracking/[redacted]/[reda
cted]?...&dzip=[...]&order_number=[...]&...

[redacted].[3pl_company].com/[redacted]/returns/step-
1?...&order=[...]&email=[...]&phone=[...]

[redacted].[3pl_company].com/[redacted]/returns?order=
[...]&bzip=[...]

[redacted].[3pl_company].com/returns/[redacted]/order/
[order_number]?...&bzip=[...]&email=[...]&phone=[...]&
...
```

Figure 10. Unencrypted URL query strings that can be used for authorizing returns

While the return process makes it simple for the consumers, an unauthorized person can start a return process to retrieve the customer's PII. Depending on the retailer, the following combination of order information can be used to initiate the return of a merchandise:

- Order number and ZIP code
- Order number and email address
- Email address and ZIP code



Track an Order or Start a Return

To **track your order** or start an **online return**, enter your info below.

Order Number or Email Address*

Shipping or Billing ZIP Code*

Returns

Enter your order number and email below to get started.

Need help finding your order number?

Order Number

Email

Returns

Enter your order information to get started.

Need help finding your order number?

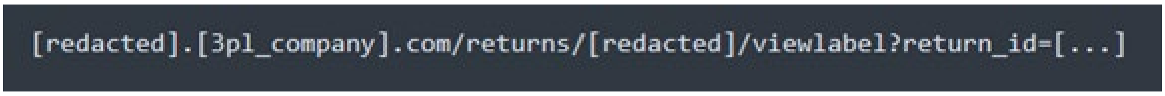
Order Number

Billing Zip Code

Figure 11. Web form pages for returning merchandise

Another flaw that we found is not in the information chosen by the developers as authentication strings since it makes the return process easy by design. Instead, the flaw was found in the way the authentication strings are sent to the server, which is through the HTTP Get method. This means that all authentication strings are visible through URL parameters and anyone who has the information can log in to the returns page. This is evident from the URL parameters shown on Figure 10, which contain authentication strings on the URL parameters for the returns page. Typically, HTTP Post is the preferred method when sending form data as compared to HTTP Get, which was evident in this case.

Once users are logged in on the returns page, they can now view what has been bought on that order without viewing the customers' PII. The final step to retrieve the name and address of the customer is to initiate a return on a merchandise and download the return shipping label and invoice. While checking the download URL for the return label and invoice, we noticed that there is no measure to check session cookies, and anyone who has the link for the label can download them.



```
[redacted].[3pl_company].com/returns/[redacted]/viewlabel?return_id=[...]
```

Figure 12. URL pattern to view the return label containing customer information

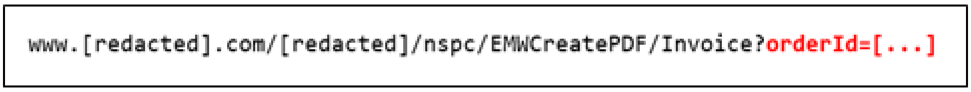
Even though it takes many steps to accomplish the return process before personal information about the consumer can be retrieved, this can easily be automated to obtain sensitive information. Also, the shipping labels created from the return spawn more opportunities for other scams that can be carried out, which will be discussed in a later section describing fake return fraud.

Also noteworthy is that not all retailers using this 3PL company are affected by the security flaw mentioned previously. We have seen an implementation that encrypts URL parameters of tracking URLs that some retailers already rolled out to prevent the leakage of order information that can initiate returns. However, the implementation for authenticating users on the returns page still uses the HTTP Get method, which still exposes the authentication strings.

Unauthorized Download of Order Invoice

An invoice for purchased merchandise is another way a customer's PII might be leaked. There are several ways e-commerce websites can provide invoices, but the most common method is by providing a download link for the PDF version of the invoice. Often, users need to log in to an account to access the order information page.

However, we found an e-commerce website's order status page that does not require any authentication to view the order summary. While the order information does not show any personal information about the buyer, downloading the invoice through a link from the webpage will reveal the address of the person who bought the merchandise from the e-commerce store.



```
www.[redacted].com/[redacted]/nspc/EMWCreatePDF/Invoice?orderId=[...]
```

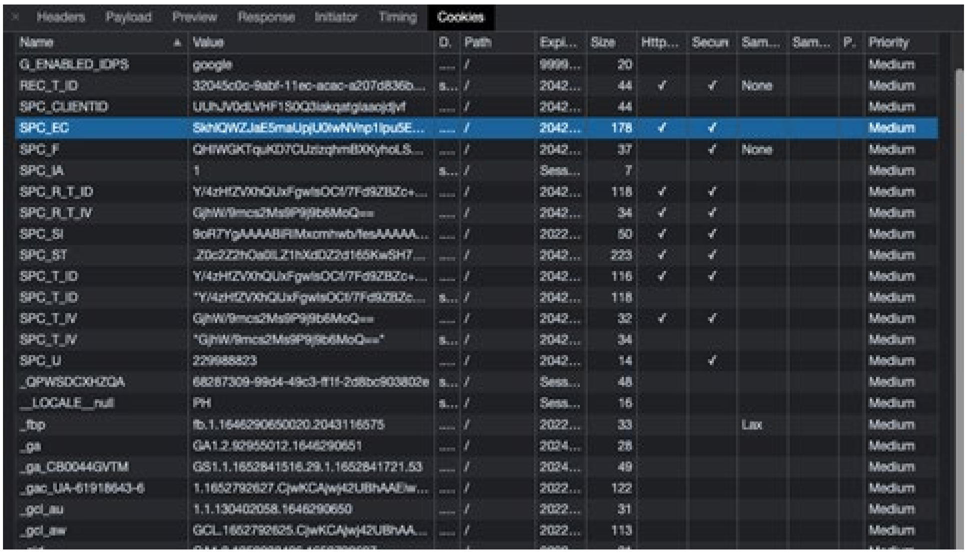
Figure 13. URL pattern to download an invoice containing customer information

Another flaw that we discovered is that directly downloading the PDF version of an invoice can be accomplished by providing the order number on the URL parameter. Session cookies should be checked before allowing users to download the invoice to verify that the actual buyer is the person authorized to download the invoice. Any unauthorized individual can therefore download the invoice and obtain the PII of customers because there is no measure in place to check the session cookies.

Order numbers can be retrieved through the URL links that are initially sent out through emails or can be brute forced by generating the order number pattern.

Session and Cookies With Expiration Set Beyond Recommended Duration

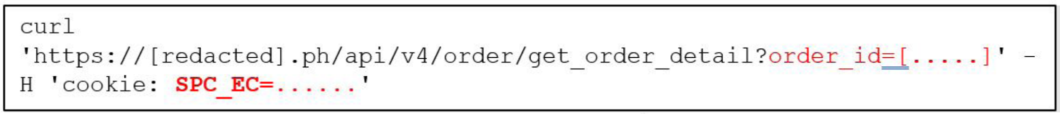
When accessing data from another server or its own, some platforms use sessions and cookies to regulate authentication. This solution follows the Open Web Application Security Project's (OWASP) good practices,[15] although session time to live (TTL) should always expire as soon as the transaction is completed or right after the user quits the connection. A normal session timeout, which terminates the session or cookie if no user interaction is detected, is two to five minutes of inactivity. The standard cookie TTL is 24 hours, which allows the user to easily access the site again. We have come across a certain 3PL that does not adhere to session and cookie expiration best practices.



Name	Value	D.	Path	Expi...	Size	Http...	Secure	Sam...	Sam...	P.	Priority
G_ENABLED_IDPS	google	....	/	9999...	20						Medium
REC_T_ID	32045c0c-9abf-11ec-acac-a207d836b...	s...	/	2042...	44	✓	✓	None			Medium
SPC_CLIENTID	UUhJV0dLVHF1S0Q3akqatglaaojdjvf	....	/	2042...	44						Medium
SPC_EC	SkhlQWZJaE5maUpjU0lwNVnp1lpu5E...	....	/	2042...	178	✓	✓				Medium
SPC_F	QHIWGKTquKD7CUzlzqhmBXKyhoLS...	....	/	2042...	37		✓	None			Medium
SPC_IA	1	s...	/	Sess...	7						Medium
SPC_R_T_ID	Y/4zHfZVXhQUxFgwlsOCl/7Fd9ZBZc+...	....	/	2042...	118	✓	✓				Medium
SPC_R_T_IV	GjhW/9mcs2Ms9P9j9b6MoQ==	....	/	2042...	34	✓	✓				Medium
SPC_SI	9oR7YgAAAABiRlMxcmhwb/fesAAAAA...	....	/	2022...	50	✓	✓				Medium
SPC_ST	.Z0c2Z2hOa0lLZ1hXdDZ2d165KwSH7...	....	/	2042...	223	✓	✓				Medium
SPC_T_ID	Y/4zHfZVXhQUxFgwlsOCl/7Fd9ZBZc+...	....	/	2042...	116	✓	✓				Medium
SPC_T_ID	"Y/4zHfZVXhQUxFgwlsOCl/7Fd9ZBZc...	s...	/	2042...	118						Medium
SPC_T_IV	GjhW/9mcs2Ms9P9j9b6MoQ==	....	/	2042...	32	✓	✓				Medium
SPC_T_IV	"GjhW/9mcs2Ms9P9j9b6MoQ=="	s...	/	2042...	34						Medium
SPC_U	229988823	....	/	2042...	14		✓				Medium
_QPWSDCXHZQA	68287309-99d4-49c3-ff1f-2d8bc903802e	s...	/	Sess...	48						Medium
__LOCALE__null	PH	s...	/	Sess...	16						Medium
_fbp	fb.1.1646290650020.2043116575	....	/	2022...	33			Lax			Medium
_ga	GA1.2.92955012.1646290651	....	/	2024...	28						Medium
_ga_CB0044GVTM	GS1.1.1652841516.29.1.1652841721.53	....	/	2024...	49						Medium
_gac_UA-61918643-6	1.1652792627.CjwKCAjwj42UBhAAEiw...	....	/	2022...	122						Medium
_gcl_au	1.1.130402058.1646290650	....	/	2022...	31						Medium
_gcl_aw	GCL.1652792625.CjwKCAjwj42UBhAA...	....	/	2022...	113						Medium

Figure 14. List of cookies that malicious actors can use to gain API access

Figure 14 shows that there is a lot of cookie information that can be used to authenticate API access. It is only a matter of testing each key to figure out which one is used to send authentication tokens to gain API access.



```
curl
'https://[redacted].ph/api/v4/order/get_order_detail?order_id=[.....]' -
H 'cookie: SPC_EC=......'
```

Figure 15. Sample curl command

After determining the suitable cookie to use for authentication, malicious actors can begin using the API to obtain more information about the user, such as phone numbers and home address, as shown in Figure 15. The cookie expiration was longer than a week, contrary to OWASP’s recommended practice. The users’ PII is clearly not protected, as cybercriminals can duplicate a transaction or make an API call for more than a week using the same cookie information.

Malicious actors can utilize the detected cookie key to replay transactions and obtain users’ personal information, which they can exploit to carry out malicious acts.

Impact of PII Leakage

Policies and Compliance

Customer information is collected during the shopping and checkout process. This information typically includes a name, physical address, email address, phone number, and payment information. Additional data such as IP address, cookie data, and browser data may also be collected. Depending on the location of the customer and the e-commerce vendor, the 3PL and 4PL providers, different laws apply to the privacy and handling of the data.

EU citizens have some form of protection provided by the General Data Protection Regulation (GDPR) that requires companies to notify customers of personal data breaches within a certain timeframe and generally requires mechanisms of protection to be in place to safeguard personal data. These regulations are enforced with heavy fines.

Canada implements the Personal Information Protection and Electronic Documents Act (PIPEDA) which contains similar forms of protection for its citizens. PIPEDA is enforced by the Office of the Federal Privacy Commissioner (FPC) and typically tries to work with companies that are violating PIPEDA to make them compliant. The FPC can fine companies that do not comply, but the fines are much lower than the fines imposed by the GDPR.

The United States of America enacted some laws that require the government to handle PII with care and perform notifications if a breach has occurred, but there are only a few laws that require private companies to protect or notify customers. The government allows some exception to specific sectors, like the financial and medical industries, which require data protection and notification. Some states have adopted or are adopting laws to increase consumer privacy. One such example is the California Consumer Protection Act, which requires safeguards and consumer notification. As shown in the following examples, some countries around the world only have a few requirements (or none at all) for companies to protect the personal data of their customers while others impose strong protections with hefty fines.

Depending on the products of the e-commerce vendor, additional care must be taken. If the products contain medical supplies or indicate the political affiliation or the sexual orientation of the customer, such information is considered protected private data under the GDPR, and possibly the laws of other countries.

Data Privacy Concerns and Impact

The e-commerce websites of firearm and firearm accessory stores, political merchandise stores, medical supplies stores, adult stores, and CDB (Cannabidiol) stores are examples of sites that might have additional privacy concerns. The privacy concerns can be attributed to laws like the GDPR, which requires medical information, political affiliation, or sexual orientation to remain private. The other privacy concerns reflect the customers' desire to keep the details of orders private for personal safety, government overreach, or difficulties at work if purchase information is known by other employees or by management which might cause embarrassment, harassment, or worse, termination of employment.

Customers of online adult stores are typically privacy-conscious individuals given the personal nature of their purchases. Online adult stores often ship items in discreet packaging so that the person delivering the package would not know it contains adult material. Some of the privacy concerns for customers of adult stores are that the shipment might reveal sexual orientation, which could be an issue within the person's household, or it could be a GDPR issue if the person is based in the EU. Additionally, there may be concerns about public disclosure for revenge or humiliation purposes and it could lead to employers punishing or terminating employees.

In the United States, firearms, firearm parts, and ammunition can be ordered online. Firearms are not sent directly to the customer; they are sent to a local dealer where the customer can pick up the firearm after a background check is done. Firearm parts, tools, and ammunition can be sent directly to a customer's home in most states. Customers who are interested in firearms are typically privacy conscious. In addition to the privacy concerns, firearms parts, tools, and ammunition can be very expensive.

The privacy concerns for the aforementioned types of customers may include government agencies collecting data, employers penalizing or terminating employees, and criminals targeting homes with firearms, which is one of the primary methods for criminals to gain access to firearms.

While CBD products are legal in most US states, there is still some stigma attached to the use of CBD products. The inadvertent exposure of a CBD purchase might affect an employee's reputation or status within the company, and, depending on the nature of the profession, might trigger an employer's drug test requirements.

Potential Attacks Enabled by PII Leakage

The retail industry has seen its fair share of fraud and scams, which affect both the merchants and consumers regardless of whether the sale is done in a physical, online, or multi-channel environment. In this section, we explore how the leakage PII and order information can be potentially used to aid fraud and scams. To the best of our knowledge, the scenarios that will be discussed have not happened yet, but we identified a few fraudulent schemes that will be greatly aided if malicious actors use the exposed PII and order information to their advantage.

Fake Return Fraud

We have identified two possible types of fraud that might occur because of the way a 3PL provider includes order identification on the URL parameters. These types of malicious activities are based on previously reported incidents of fraud and may comprise a subset of possible fraud. Both examples can negatively affect the merchants.

Unlike a previously reported scam in which the buyer was alleged to have defrauded a popular online retailer by obtaining US$370,000 for returned items,[16] the first type of return fraud is a nuisance fraud in which a third party finds the order link that was accessed by the customer. The third party initiates the return process, receives a return label, then puts rocks, bricks, or some other heavy and inexpensive item in a box, seals the box, attaches the return label, and drops the box off at a shipping location. Bear in mind that the third party involved does not earn anything from this fraud and can only cause nuisance to the merchant. The merchant typically pays for and processes the return, only to find rocks placed inside the return package. In addition to the cost of shipping the item, there is also manpower cost for dealing with the fake return. This can also strain the relationship between the merchant and the customer.

According to Brian Lim, founder and CEO of INTO THE AM, “the biggest challenge for reverse logistics is the sheer amount of time it takes to process one return versus shipping out one order. It takes at least two to three times the amount of time. This challenge is exacerbated by labor shortages in our warehouse team.”[17]

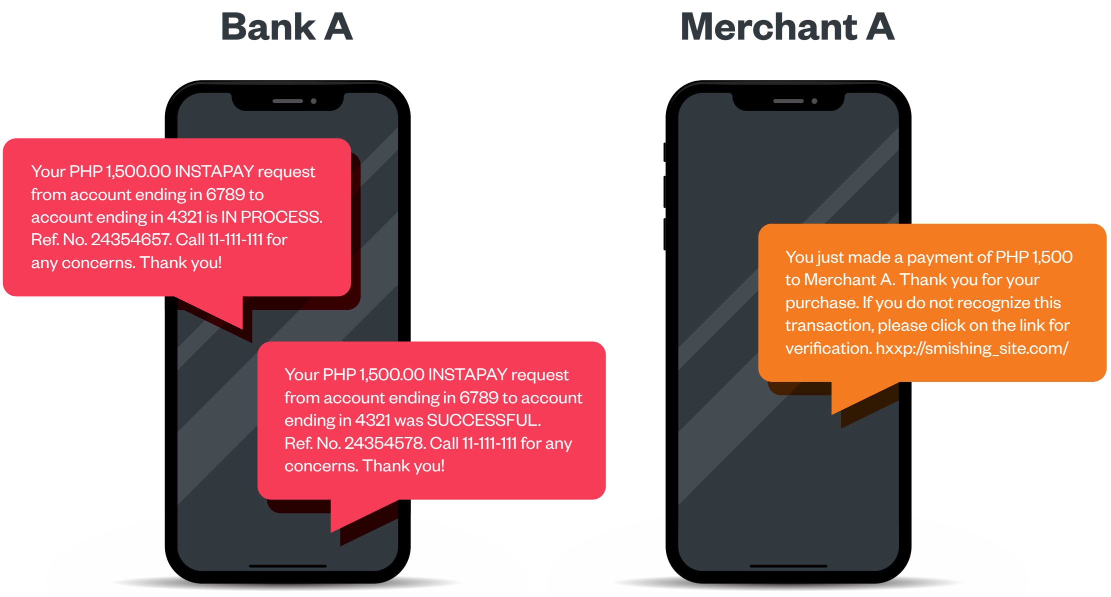
The second example of fraud involves a combination of cyber and physical vectors. A third party can perform the following procedure to carry out this fraud:

1. The third party finds the order link that was accessed by the customer.
2. He prints out the receipt.
3. He goes to a brick-and-mortar store.
4. He takes one or more of the same items that was bought online off the shelf.
5. He brings the item(s) and receipt to customer service to initiate the return

We performed a legitimate version of this type of scheme by returning an item that we ordered online personally to the physical store. We presented the item and the order number to the sales attendant. The item was returned, and we were issued store credit. No ID, original credit card, or other information was required; providing them the order number sufficed.

Fraud and Phishing

Information such as phone numbers, email addresses, and purchase methods can be used to perform SMS fraud and phishing attacks. Criminals can analyze the users' buying habits and mode of payment and craft sophisticated SMS messages or phishing websites that indicate the purchase order. Figure 16 shows two different images. The one on the left is a sample of a legitimate SMS transaction notification from the vendor sent upon payment of an order, while the image on the right shows a sample of a fraudulent SMS notification from an unknown sender. Malicious actors can deceive consumers by setting the sender's name to one that closely resembles a legitimate merchant's name. The message from the malicious SMS notification indicates a transaction amount with instructions to access the link provided to verify it in case the recipient did not make the purchase. The link redirects the user to a phishing website that collects sensitive information.



Your PHP 1,500.00 INSTAPAY request from account ending in 6789 to account ending in 4321 is IN PROCESS. Ref. No. 24354657. Call 11-111-111 for any concerns. Thank you!

Your PHP 1,500.00 INSTAPAY request from account ending in 6789 to account ending in 4321 was SUCCESSFUL. Ref. No. 24354578. Call 11-111-111 for any concerns. Thank you!

You just made a payment of PHP 1,500 to Merchant A. Thank you for your purchase. If you do not recognize this transaction, please click on the link for verification. hxxp://smishing_site.com/

Figure 16. A sample SMS notification for a legitimate transaction (left) and a sample of a fraudulent SMS message that redirects to a phishing website (right)

This is an example of a phishing attack via SMS that is currently being done by criminals in a "spray and pray" scheme that involves sending phishing SMS to as many phone numbers as possible and praying that someone falls for it. However, if attackers can identify that person X with phone number 12345678 has ordered an item from online store ABC through leaked PII, they can use these details to enhance the social engineering tactics and timing of their SMS phishing attacks such that the details of the purchase match what the customer is expecting, thus increasing the likelihood that the target falls for the phishing attack.

Intercept/Delivery Scam

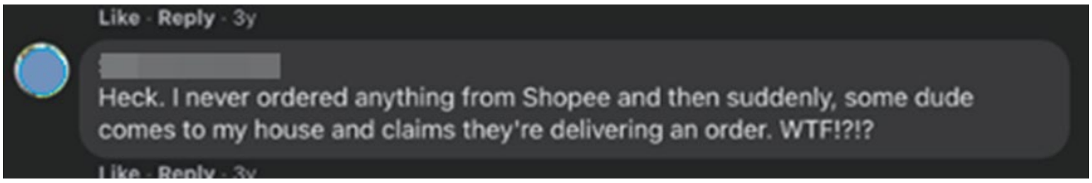
Leakage of customers' PII from poorly implemented web or API authentication can open new avenues for criminals to formulate new scams or improve existing ones. The increase of online purchases during the pandemic saw a similar increase of scams and fraud for e-commerce businesses.[18] Scams like package interception, also known as cash-on-delivery scams, became rampant in Southeast Asia. A cash-on-delivery scam involves a malicious actor delivering a low-cost item priced between US$5 to $10 to a customer, with the delivery personnel claiming cash-on-delivery as the mode of payment. In this case, the low-cost item is marked up several times over, such that the $5 to $10 item gets sold for $20 to $60. The package has the customer's name on it, but as expected, the customer has no memory of having ordered it because no order was made in the first place. The customer is then tricked into paying the purported price of the item. How does this scam work? Attackers gather information using the following means:

1. Collection of the customers' information that they make publicly available online such as through social media platforms
2. Use of improperly disposed packaging that still has the recipient's personal details legibly printed on the package label
3. Collection of information by a rogue employee of the delivery partner who is part of the scam

Several reported cases of fraud had been published on the internet.

One report described a type of social engineering scheme in which a courier of the logistics provider delivers an item that the customer purportedly bought.[19] Given that cash-on-delivery is a popular mode of payment in many e-commerce platforms, the courier then persuasively asks that the customer pay an amount ranging from US$20 to $50. Customers victimized by this scheme have no recollection of ever ordering the item as the order was never made in the first place. Those who fell prey to the scam were shocked to find inexpensive items when they unwrapped the parcel, realizing that they cost only about $15 or even less. The report also noted that the collection of the victims' PII and observed patterns in their buying habits by the malicious actors most likely enabled the scam. The fraudsters went to the extent of using counterfeit package labels and procuring the cheap merchandise to make the ruse believable.

Another report was of scammers that collect customers' PII from improperly thrown delivery packages.[20] The Royal Malaysia Police warned the public of malicious actors that harvest PII, which they use to launch their schemes. The report mentioned a viral video of an unidentified fraudster that was shown to be gathering the name, phone number, and home address of a potential victim from a delivery package that was disposed in a public trash bin. The malicious actor used the private information to persistently contact the victim to extort money. The report also stated that the scammer later impersonated a delivery personnel who went to the victim's home and demanded payment for a purchase that was allegedly not yet paid. Part of the scammer's modus operandi to convince the victim's family into paying was by making them scan a barcode before handing the payment over to the malicious actor.



Like · Reply · 3y

[redacted]

Heck. I never ordered anything from Shopee and then suddenly, some dude comes to my house and claims they're delivering an order. WTF!?!?

Like · Reply · 3y

Figure 17. Sample social media post of a scam target retrieved from a popular social networking website

A common variable that can be observed in the aforementioned cases is the delivery of packages by fraudsters that the customer didn't purchase, with the intent of extorting money from the victim.

The scams are enabled by improperly disposed packaging labels. Delivery packaging labels contain the recipient's details and online store information. This gives scammers the necessary information to identify people who use e-commerce and target them for the scam. Therefore, the security mechanism to prevent such scams is to properly dispose the delivery packaging by making the information in the labels unreadable. This can be done by shredding the label, marking the label out using blackout pens, or by using heat guns on labels printed on thermal paper.

Similarly, PII and order information leaked through APIs can be used to perform the same scam. This is why, aside from e-commerce platforms fixing the security and authentication flaws, users should also practice online shopping security hygiene by clearing the cache and making sure the password saving feature is not used. While this does not completely solve the problem, it will help minimize the exposure of PII.

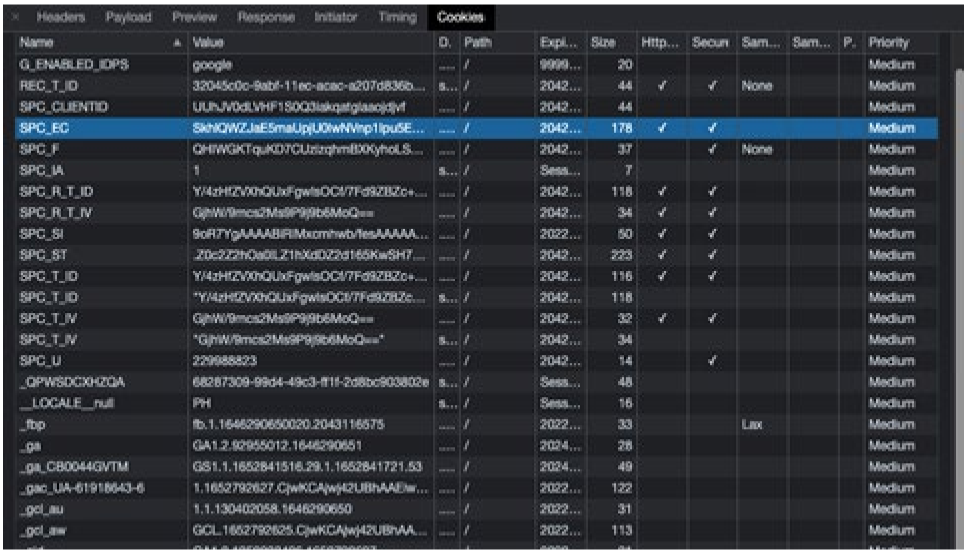
Addressing Unsecure Coding Practices That Lead to PII Leakage

APIs are widely used to carry out data transactions between platforms and systems belonging to the same entity or when companies in the supply chain integrate services or solutions. Using APIs for different transactions, such as data query or posting, should be done with caution. Basic API queries such as retrieving the most recent weather data, the current foreign exchange rate, or a search query, do not require full security.

To summarize, utilizing an API to access publicly available data does not require complete security as the data is not sensitive, personal, or proprietary. Considering that personal information (such as one's name, age, birthday, and address) and vital information (such as the telemetry data from a device) can be exploited for malevolent purposes. Therefore, they must be protected through secure connection and data encryption. In this section, we will elaborate on what we consider to be typical unsecure coding habits that lead to PII leakage as well as secure coding practices to prevent them from occurring, which, in fact, have already been in place thanks to security recommendations that that the OWASP released five to 10 years ago.

Session and Cookie Expiration

Session expiration determines when a user session's authenticated connection to the server is terminated. By default, it is set to one day or the session is terminated after users quit their connection to the site. The same mechanism applies to cookie expiration.



Name	Value	D.	Path	Expi...	Size	Http...	Secure	Sam...	Sam...	P.	Priority
G_ENABLED_IDPS	google	....	/	9999...	20						Medium
REC_T_ID	32045c0c-9abf-11ec-acac-a207d836b...	s...	/	2042...	44	✓	✓	None			Medium
SPC_CLIENTID	UUhJV0dLVHF1S0Q3iakqatglaaojdjvf	....	/	2042...	44						Medium
SPC_EC	SkhlQWZJaE5maUpjU0lwNVnp1lpuSE...	....	/	2042...	178	✓	✓				Medium
SPC_F	QHIWGKTquKD7CUzizqhmBXKyhoLS...	....	/	2042...	37		✓	None			Medium
SPC_IA	1	s...	/	Sess...	7						Medium
SPC_R_T_ID	Y/4zHfZVXhQUxFgwlsOCl/7Fd9ZBZc+...	....	/	2042...	118	✓	✓				Medium
SPC_R_T_IV	GjhW/9mcs2Ms9P9j9b6MoQ==	....	/	2042...	34	✓	✓				Medium
SPC_SI	9oR7YgAAAABlRlMxcmhwb/lesAAAAA...	....	/	2022...	50	✓	✓				Medium
SPC_ST	.Z0c2Z2hOa0lLZ1hXdDZ2d165KwSH7...	....	/	2042...	223	✓	✓				Medium
SPC_T_ID	Y/4zHfZVXhQUxFgwlsOCl/7Fd9ZBZc+...	....	/	2042...	116	✓	✓				Medium
SPC_T_ID	"Y/4zHfZVXhQUxFgwlsOCl/7Fd9ZBZc...	s...	/	2042...	118						Medium
SPC_T_IV	GjhW/9mcs2Ms9P9j9b6MoQ==	....	/	2042...	32	✓	✓				Medium
SPC_T_IV	"GjhW/9mcs2Ms9P9j9b6MoQ=="	s...	/	2042...	34						Medium
SPC_U	229988823	....	/	2042...	14		✓				Medium
_QPWSDCXHZQA	68287309-99d4-49c3-ff1f-2d8bc903802e	s...	/	Sess...	48						Medium
__LOCALE__null	PH	s...	/	Sess...	16						Medium
_fbp	fb.1.1646290650020.2043116575	....	/	2022...	33			Lax			Medium
_ga	GA1.2.92955012.1646290651	....	/	2024...	28						Medium
_ga_CB0044GVTM	GS1.1.1652841516.29.1.1652841721.53	....	/	2024...	49						Medium
_gac_UA-61918643-6	1.1652792627.CjwKCAjwj42UBhAAEiw...	....	/	2022...	122						Medium
_gcl_au	1.1.130402058.1646290650	....	/	2022...	31						Medium
_gcl_aw	GCL.1652792625.CjwKCAjwj42UBhAA...	....	/	2022...	113						Medium

Figure 18. The list shows cookies with expiration dates set beyond the OWASP-recommended duration, thus making the cookie information available for malicious actors to replay a transaction.

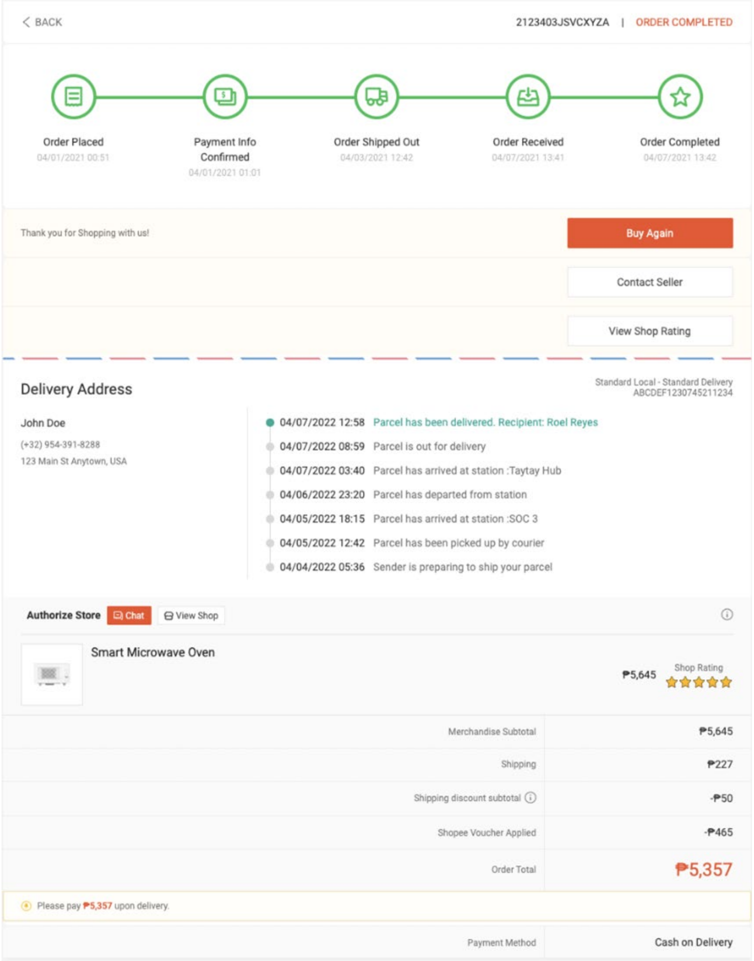
```
curl
'https://[redacted].ph/api/v4/order/get_order_detail?order_id=[....]'
-H 'cookie:
SPC_EC=cHFISEZDU2wydmJQWFFESHF4L3kwRlNFcl6YRnIfCOpgYu45uojhB6n3ps+o+2
Xhj0VdWPwo9K.....'
```

Figure 19. Replicating a transaction via curl using the exposed cookie information

If a cookie or session key value is required for data exchanges between a host and a server, ensure that the key's expiration time is kept to a minimum of two to five minutes or even less depending on the information and high-risk data involved. If possible, the key's lifespan for token authentication stored in cookies should be less than a minute. The reason for this is to prevent such keys from being reused to obtain access to the users' personal information. Session timeout should be activated once the user is no longer performing any action on the website to prevent expired cookies from being reused.[21]

Excessive Data Exposure

Excessive data exposure occurs when more data than is needed is exposed. Some developer implementations send all the information of a transaction rather than what is just needed to complete the transaction. This creates a situation in which data is exposed to accounts with access restrictions or limited privileges. In the case of leaking logistics data, excessive information can be used to monitor the buying habits of users. It also exposes information that can be exploited for scams or fraud.



2123403JSVCXYZA | ORDER COMPLETED

Order Placed	Payment Info Confirmed	Order Shipped Out	Order Received	Order Completed
04/01/2021 00:51	04/01/2021 01:01	04/03/2021 12:42	04/07/2021 13:41	04/07/2021 13:42

Thank you for Shopping with us!

Delivery Address

Standard Local - Standard Delivery
ABCDEF1230745211234

John Doe
(+32) 954-391-8288
123 Main St Anytown, USA

04/07/2022 12:58	Parcel has been delivered. Recipient: Roel Reyes
04/07/2022 08:59	Parcel is out for delivery
04/07/2022 03:40	Parcel has arrived at station :Taytay Hub
04/06/2022 23:20	Parcel has departed from station
04/05/2022 18:15	Parcel has arrived at station :SOC 3
04/05/2022 12:42	Parcel has been picked up by courier
04/04/2022 05:36	Sender is preparing to ship your parcel

Authorize Store

Smart Microwave Oven ₱5,645

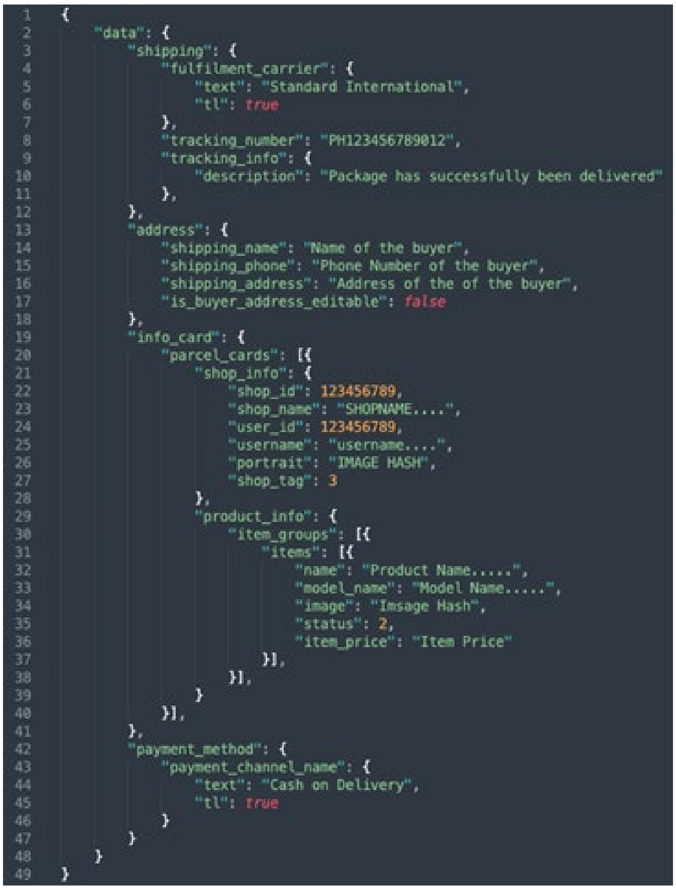
Shop Rating ★★★★★

Merchandise Subtotal	₱5,645
Shipping	₱227
Shipping discount subtotal	-₱50
Shopee Voucher Applied	-₱465
Order Total	₱5,357

Please pay ₱5,357 upon delivery.

Payment Method	Cash on Delivery

Figure 20. Transaction via user interface (UI)



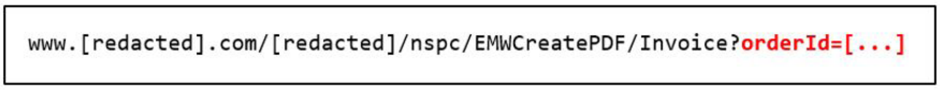
```
{
    "data": {
        "shipping": {
            "fulfilment_carrier": {
                "text": "Standard International",
                "tl": true
            },
            "tracking_number": "PH123456789012",
            "tracking_info": {
                "description": "Package has successfully been delivered"
            },
        },
        "address": {
            "shipping_name": "Name of the buyer",
            "shipping_phone": "Phone Number of the buyer",
            "shipping_address": "Address of the of the buyer",
            "is_buyer_address_editable": false
        },
        "info_card": {
            "parcel_cards": [{
                "shop_info": {
                    "shop_id": 123456789,
                    "shop_name": "SHOPNAME....",
                    "user_id": 123456789,
                    "username": "username....",
                    "portrait": "IMAGE HASH",
                    "shop_tag": 3
                },
                "product_info": {
                    "item_groups": [{
                        "items": [{
                            "name": "Product Name.....",
                            "model_name": "Model Name.....",
                            "image": "Imsage Hash",
                            "status": 2,
                            "item_price": "Item Price"
                        }],
                    }],
                }
            }],
        },
        "payment_method": {
            "payment_channel_name": {
                "text": "Cash on Delivery",
                "tl": true
            }
        }
    }
}
```

Figure 21. Exposing excessive information from an API response

How do we prevent excessive data exposure? When passing data from one server to another, the return data from API requests should only contain data that is limited based on the server's requirements. We have encountered API calls that return all of the users' data, but the question is whether all the data is required by the server to accomplish its mission. This is a question that the developers who integrate the application's call to another vendor must answer. A recommended strategy is to determine which data is required to complete the transaction. If the customers' information is required, determine what data is needed and classify it as high-risk or not.[22] It is not an innovative idea to return all of the users' information so that the connecting application does not have to make a separate API call to request additional information. While this method optimizes calls, it does so at the risk of exposing all of the sensitive information, which makes it vulnerable to accidental data leakage or data harvesting by malicious actors.

Broken Object Level Authorization

Object level authorization is an access control strategy that is typically implemented at the code level to ensure that access to objects is given only to authorized users. Object level authorization checks should be implemented in every API endpoint that receives an object's ID and performs any type of operation on the object. The tests should ensure that the logged-in user has permission to perform the operation on the requested object. An example of this was discussed in a prior section in this paper titled, “Unauthorized Download of Order Invoice” for e-commerce retailers.



```
www.[redacted].com/[redacted]/nspc/EMWCreatePDF/Invoice?orderId=[...]
```

Figure 22. URL pattern to download an invoice containing customer PII

Users’ PII should be protected by encrypting the data or requiring user authentication before being accessed. When using 3PL API Integrations, PII data should be protected and secured when it is shared with 3PL-affiliated suppliers. There are several different authentication algorithms that can be used to safeguard API transactions. Requests that return critical information are the types of transactions that require authentication. Passing authentication from the websites that require users to authenticate via login portals and using that authentication to execute backend calls is a standard approach to securing API calls.[23] However, this is occasionally overlooked. APIs are used to access a backend database to obtain specific information needed to complete a transaction or render data to a website’s UI. Tokens such as JSON Web Token (JWT)[24] or custom tokens generated using base64 encoded with salt,[25] are a good practice for securing API calls. These tokens can be automatically generated upon user login and stored in a cookie with a set expiration date. Tokens are regenerated every time the user logs in, and are freely accessible through web API calls.

A good API encourages developers to use it and share it, thus establishing positive feedback loops among users. Each successful implementation contributes to higher engagement and elicits more contributions from developers who add value to the service.

When designing an API, keep two things in mind: **What data should be given throughout the transaction and what authentication mechanisms should be used**. Not all system developers use authentication, especially for data that is made public via API. When transferring data containing PII with a third-party, it should always be safeguarded. Encrypt the data or provide authentication when sending this information. Authentication should be straightforward; a basic mechanism like JWT or base64 salted tokens should suffice. Other strong encryption methods, such as Advanced Encryption Standard (AES) data encryption, are also good, although encrypting and decrypting data on every call is a resource-intensive task from a server’s point-of-view.

Latency and ensuring that the data transmission does not trigger a distributed denial of service (DDoS) should also be considered. Having thousands of simultaneous connections making API call requests with authentication is an example of this. This can cause the server to use a lot of resources, which might cause the system to crash. As a result, considering the system architecture is a vital component in choosing the right kind of encryptor and authentication.

Conclusion

Given the limited movement of people during the peak of the pandemic, e-commerce provided a perfect alternative for consumers to shop. Logistics played a vital part in enabling businesses to provide essential services by ensuring that the products bought by consumers from online stores reach them in a timely manner. E-commerce platforms provided merchants a way to quickly adapt and set up online businesses easily. It also gave merchants the flexibility to integrate 3PL services that suit their business needs so that they are not limited to only what the e-commerce platforms offer.

While securing customer data is one of the primary concerns of e-commerce platforms and logistics providers to prevent PII leakage, the security flaws that the OWASP warned about more than 10 years ago can still be observed. A thorough auditing of API services and the application of encryption on URL query strings can help minimize the exposure of sensitive data.

While business owners do not have direct control over the security implementation of the e-commerce platforms and logistics services that they choose, damage to brand reputation is more than likely to arise if security flaws are not addressed and the PII of customers starts leaking. This can also dampen consumer confidence to purchase online. Depending on the consumers to safeguard their personal information might cause them to choose alternative websites that can assure their data is adequately secured.

Consumers can minimize the risk of exposing personal information by avoiding the installation of unknown browser extensions to web browsers that can read and collect unencrypted URL query strings. Using legitimate VPNs on public Wi-Fi networks can also help reduce the exposure of personal data. Consumers should also delete their browsing history especially on public or shared devices.

Implementing two-factor or multi-factor authentication for e-commerce platforms before displaying content with personal information should become a standard practice rather than relying only on redirection from URL links sent through email or SMS. This will ensure that the party making the URL request that contains PII is authorized to view it. Understanding these security flaws that are commonly overlooked can minimize the exposure of PII that cybercriminals might abuse.

Logistics APIs have become more of a necessity in the modern marketplace, therefore securing them is a must. Neglecting to do so exposes users to data leaks that enable malicious actors to devise more attacks that can inflict more harm. Keep in mind that these security flaws are not difficult to abuse, so even a low-level cybercriminal can perform them. To avoid such security risks, key stakeholders should adopt a proactive cybersecurity approach.

References

1 Katharina Buchholz. (Sept. 28, 2021). *Statista*. “The Parcel Shipping Boom Continues.” Accessed July 22, 2022 at https://www.statista.com/chart/10922/parcel-shipping-volume-and-parcel-spend-in-selected-countries/.

2 Parcel Pending. (n.d.). “Parcel Delivery Statistics.” Accessed July 22, 2022 at https://www.parcelpending.com/blog/package-delivery-statistics/.

3 Edoardo Totolo and Hemant Baijal. (Dec. 22, 2020). *World Bank Blogs*. “How a Pandemic-Induced Boom can Reshape Financial Services.” Accessed on July 22, 2022 at https://blogs.worldbank.org/psd/how-pandemic-induced-boom-e-commerce-can-reshape-financial-services.

4 Amazon. (n.d.). “Start Selling with Amazon.” Accessed on August 24, 2022 at https://www.ebay.com/help/selling/selling/start-selling-ebay?id=4081.

5 eBay Customer Service. (n.d.). “Start Seeling on eBay.” Accessed on August 24, 2022 at https://www.ebay.com/help/selling/selling/start-selling-ebay?id=4081.

6 Shopify. (n.d.). “How to Sell Online.” Accessed on August 24, 2022 at https://www.shopify.com/ph/blog/topics/sell.

7 Lazada. (n.d.). “Start Selling on the Leading E-Commerce Platform Today!” Accessed on August 24, 2022 at https://pages.lazada.com.ph/wow/i/ph/PHCampaign/ssu?hybrid=1&exlaz=d_1:mm_150050845_51350203_2010350203::11:12348389739!114642778221!how%20to%20sell%20in%20lazada!b!aud-1467503182977:kwd-301489-478384!c!!!!498716220601!&gclid=Cj0KCQjw9ZGYBhCEARIsAEUXITXhCvz7whA5sQAuqBwtAgyAC9L1Z_zqi-7oNmhv1mpdURpNJlXYii8aAkG9EALw_wcB.

8 Elise Dopson and Jessica Wynne Lockhart. (February 1, 2022). *Shopfiy Plus*. “What is 3PL: How to Select a Third-Party Logistics Partner.” Accessed on July 25, 2022 at https://www.shopify.com/enterprise/third-party-logistics-3pl.

9 Nicole Martins Ferreira. (April 20, 2022). *Oberlo*. “How to Start a Dropshipping Business in 2022.” Accessed on July 25, 2022 at https://www.oberlo.com/blog/how-to-start-a-dropshipping-business.

10 Google Support. (n.d.). “Best Practices to Avoid Sending Personally Identifiable Information.” Accessed on July 25, 2022 at https://support.google.com/analytics/answer/6366371#zippy=%2Cin-this-article.

11 Asuman Senol, Gunes Acar, and Mathias Humbert. (n.d.) “Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission.” Accessed on July 25. 2022 at https://homes.esat.kuleuven.be/~asenol/leaky-forms/leaky-forms-usenix-sec22.pdf.

12 Trend Micro Research. (Sept. 17, 2019). “The Risks of Open Banking: Are Banks and Their Customers Ready for PSD2?” Accessed on July 25, 2022 at https://www.trendmicro.com/vinfo/fi/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2.

13 Tara Seals. (Aug. 11, 2018). *Threatpost*. “DEF CON 2018: Telltale URLs Leak PIIs to Dozens of Third Parties.” Accessed on July 25, 2022 at https://threatpost.com/def-con-2018-telltale-urls-leak-pii-to-dozens-of-third-parties/134960/.

14 Robert Gilbert. (n.d.). *OWASP*. “Information Exposure Through Query Strings in URL.” Accessed on July 25, 2022 at https://owasp.org/www-community/vulnerabilities/Information_exposure_through_query_strings_in_url.

15 OWASP. (n.d.). “What is API Security?” Accessed on July 26, 2022 at https://owasp.org/www-project-api-security/.

16 Isobel Van Hagen. (Aug. 3, 2019). *Newsweek*. “22-Year-Old Allegedly Scammed Amazon Out of $370K With Return Shipments Filled With Dirt.” Accessed on August 15, 2022 at https://www.newsweek.com/22-year-old-allegedly-scammed-amazon-out-370k-return-shipments-filled-dirt-1452452.

17 Elise Dopson. (Mar. 1, 2022). *Shopify Plus*. “Reverse Logistics: How to Process Returns Quickly, Easily, and Efficiently.” Accessed on July 25, 2022 at https://www.shopify.com/enterprise/reverse-logistics.

18 Louis Columbus. (May 18, 2020). *Forbes*. “How E-Commerce’s Explosive Growth Attraacts Fraud.” Accessed on July 25, 2022 at https://www.forbes.com/sites/louiscolumbus/2020/05/18/how-e-commerces-explosive-growth-is-attracting-fraud/?sh=63c4dac6c4b9.

19 Joser Ferreras. (March 17, 2021). “The Cash-on-Delivery Scam and What You Can Learn From This Shopper’s Experience.” Accessed on July 27, 2022 at https://www.tripzilla.ph/cash-on-delivery-scam/25759/.

20 Angelin Yeoh. (Dec. 14, 2020). *The Star*. “PDRM: Scammers May Be Stealing Your Personal Info From Discarded Delivery Packages.” Accessed on July 27, 2022 at https://www.thestar.com.my/tech/tech-news/2020/12/14/pdrm-scammers-may-be-stealing-your-personal-info-from-discarded-delivery-packages.

21 OWASP. (n.d.). “Session Timeout.” Accessed on July 27, 2022 at https://owasp.org/www-community/Session_Timeout.

22 Github. (n.d.). “AP:2019 Excessive Data Exposure.” Accessed on July 27, 2022 at https://github.com/OWASP/API-Security/blob/master/2019/en/src/0xa3-excessive-data-exposure.md.

23 Amazon Web Services. (n.d.). “Security Best Practices in Amazon API Gateway.” Accessed on July 27, 2022 at https://docs.aws.amazon.com/apigateway/latest/developerguide/security-best-practices.html.

24 Amazon Web Services. (n.d.). “Controlling Access to HTTP APIs with JWT Authorizers.” Accessed on July 27, 2022 at https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-jwt-authorizer.html.

25 SaltStack. (n.d.). “Salt.Modules.Hashutil: A Collection of Hashing and Encoding Functions.” Accessed on September 2, 2022 at https://docs.saltproject.io/en/latest/ref/modules/all/salt.modules.hashutil.html.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research