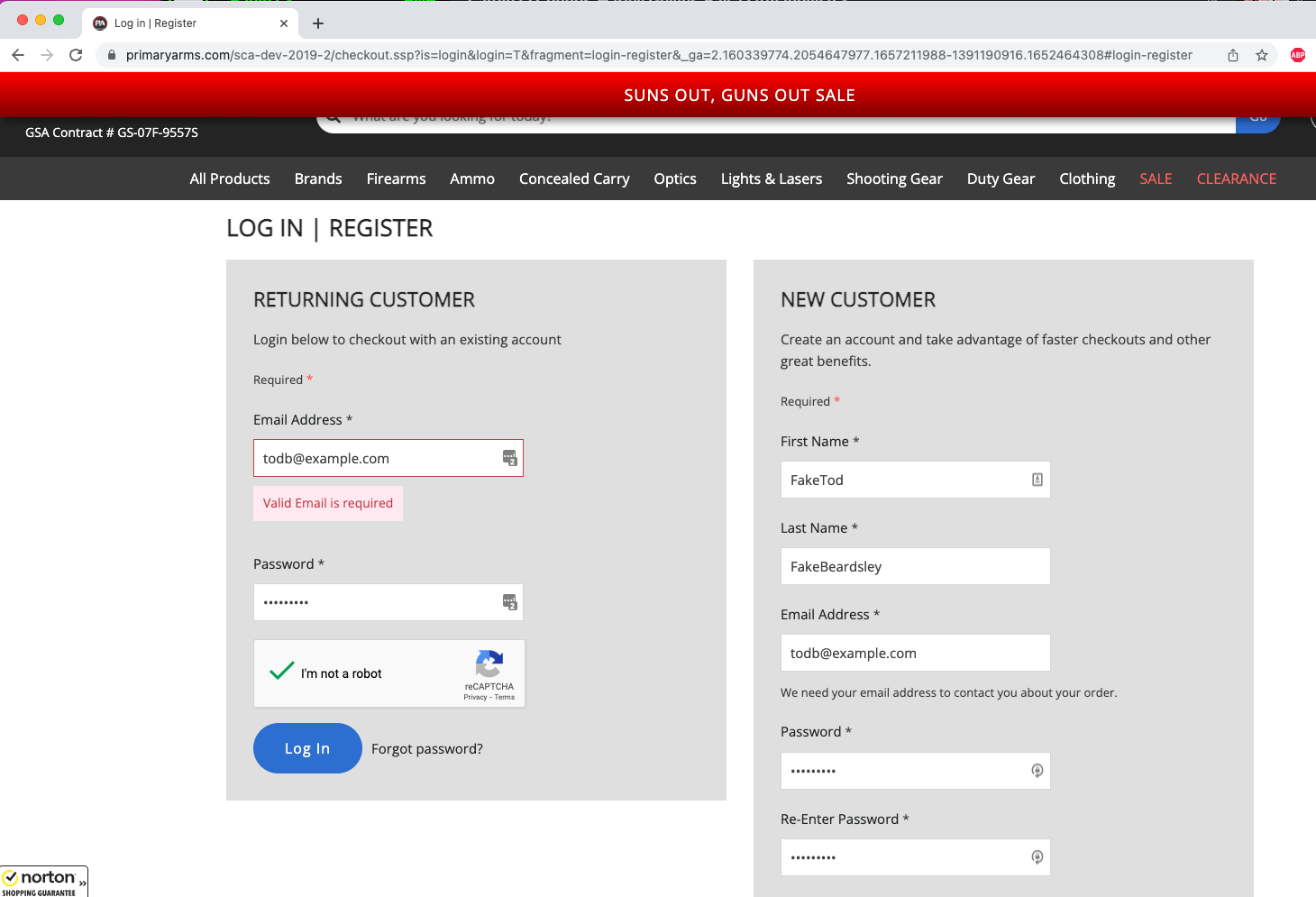
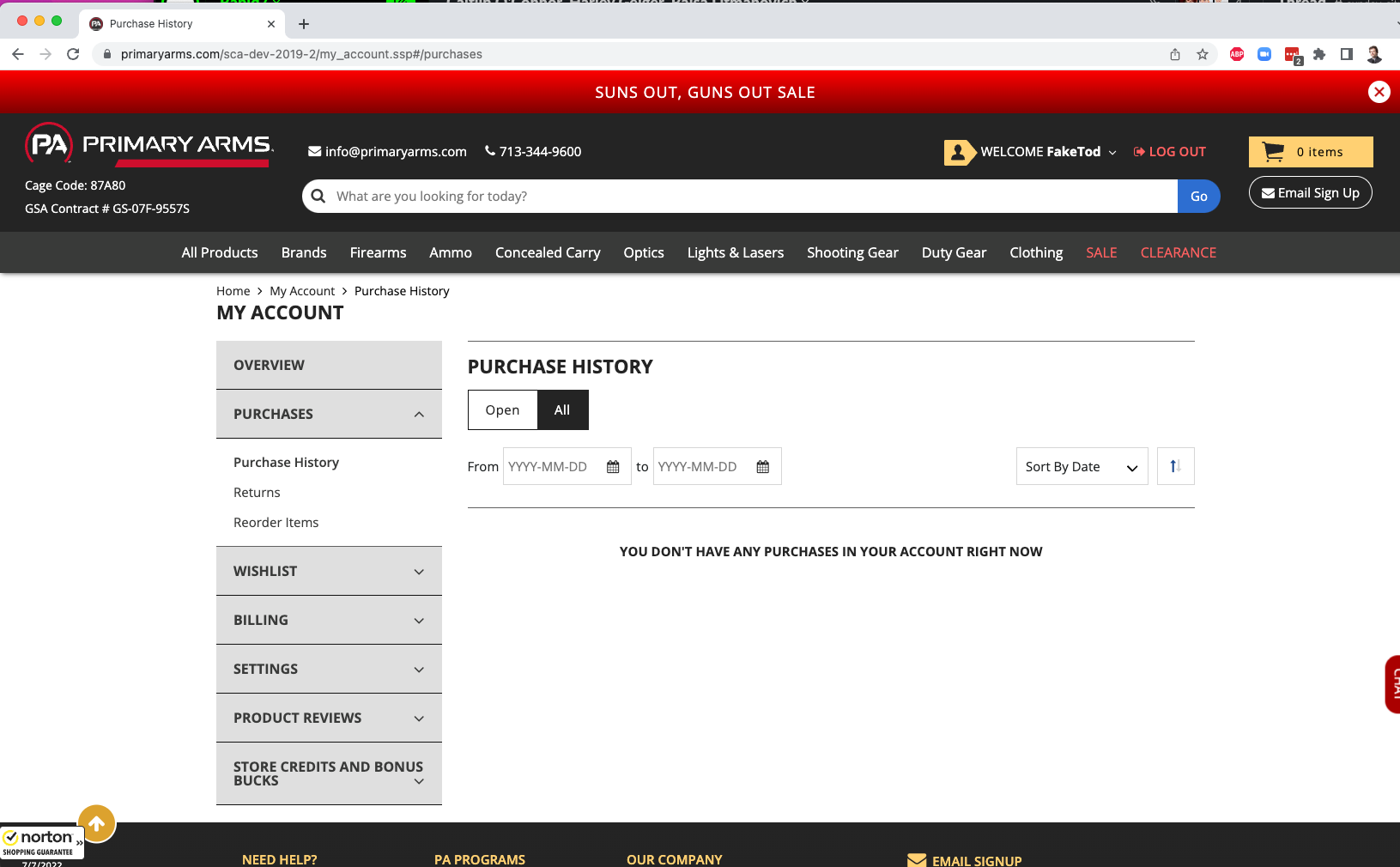
# Primary Arms PII Disclosure via IDOR (FIXED)

An authenticated user can inspect the purchase information of other Primary Arms customers by manually navigating to a known or guessed record sales order URL, as demonstrated in the series of screenshots below.

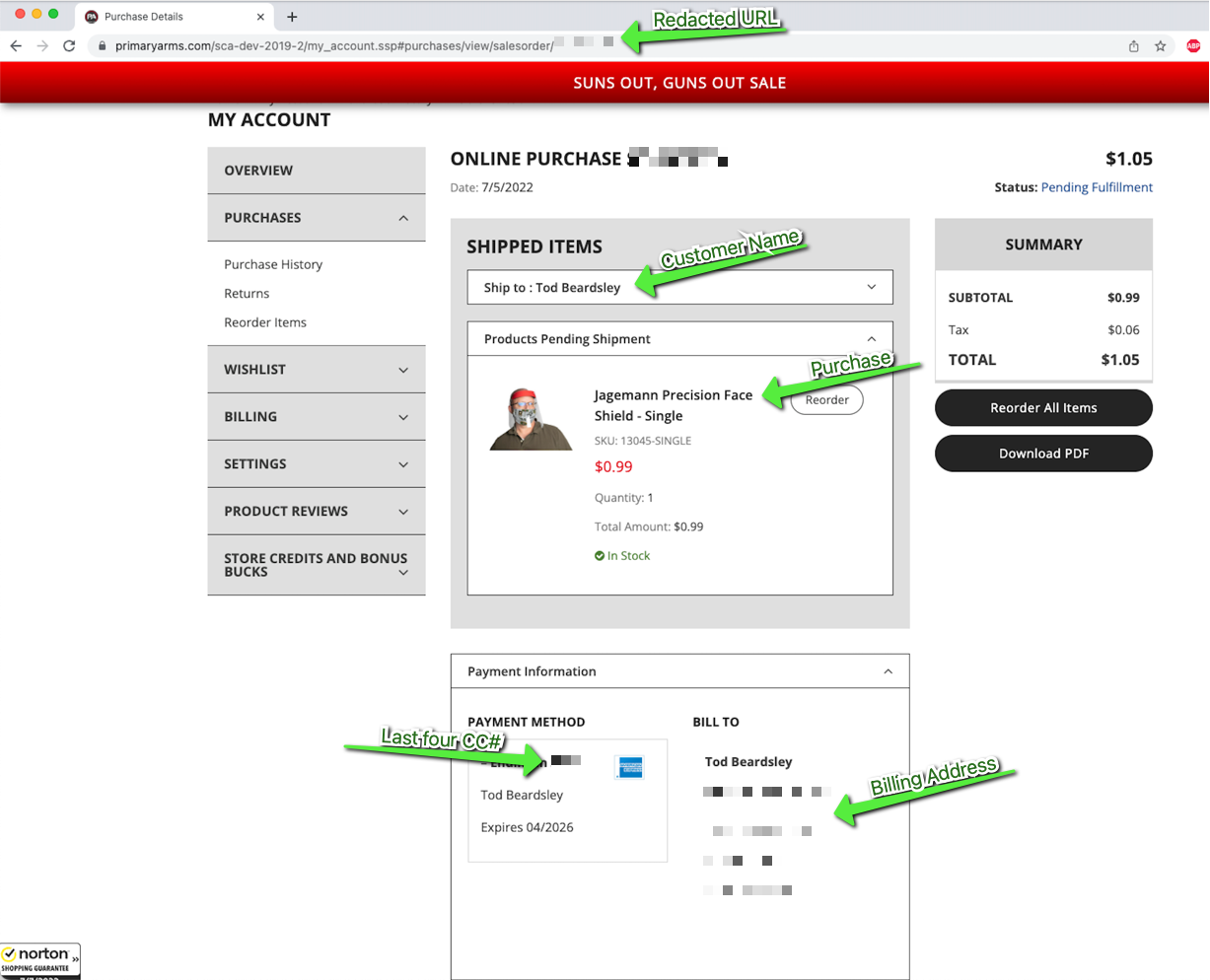
First, in order to demonstrate the vulnerability, I created an account with the username todb@example.com, which I call "FakeTod FakeBeardsley."



Note that FakeTod has no purchase history:



Next, I'll simply navigate to the URL of a real purchase, made under my "real" account. An actual attacker would need to learn or guess this URL, which may be easy or difficult (see Impact, below). The screenshot below is a (redacted) view of that sales order receipt.

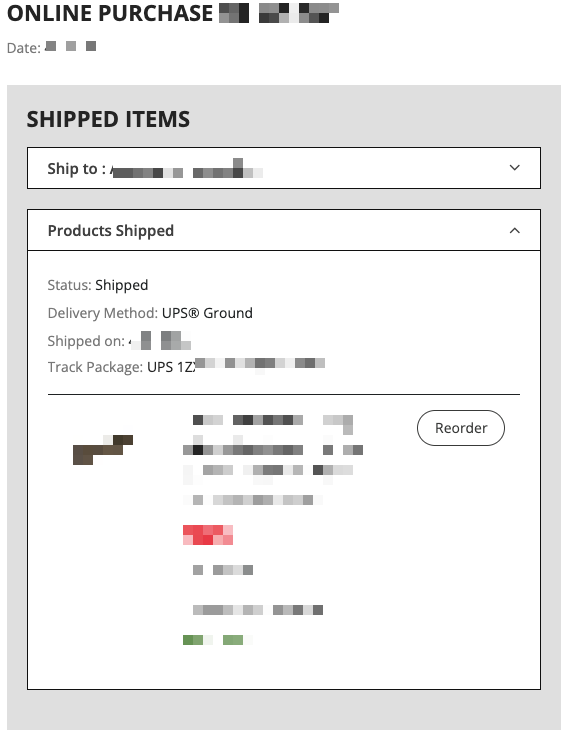


The redacted URL is hxxps://www.primaryarms.com/sca-dev-2019-2/my\_account.ssp#purchases/view/salesorder/85460532, and the final 8-digit salesorder value is the insecure direct object reference. In this case, we can see:

* Customer name
* Purchased item
* Last four digits and issuer of the credit card used
* Billing address and phone number

Manipulating this value produces other sets of PII from other customers, though the distribution is non-uniform and currently unknown (see below, under Impact, for more information).

If a given salesorder reference includes a shipped item, that tracking information is also displayed, as shown in this redacted example:



Depending on the carrier and the age of the ordered item, this tracking information could then be used to monitor and possibly intercept delivery of the shipped items.

**Root cause**

The landing page for primaryarms.com and other pages have this auto-generated comment in the HTML source:

<!-- SuiteCommerce [ prodbundle\_id "295132" ] [ baselabel "SC\_2019.2" ] [ version "2019.2.3.a" ] [ datelabel "2020.00.00" ] [ buildno "0" ] -->

<!-- 361 s: 25% #59 cache: 4% #17 -->

<!-- Host [ sh14.prod.bos ] App Version [ 2022.1.15.30433 ] -->

<!-- COMPID [ 3901023 ] URL [ /s.nl ] Time [ Mon Jul 11 09:33:51 PDT 2022 ] -->

<!-- Not logging slowest SQL -->

This indicates a somewhat old version of SuiteCommerce, from 2019, being run in production. It's hard to say for sure that this is the culprit of the issue, or even if this comment is accurate, but our colleagues at CERT/CC noticed that NetSuite released an update in 2020 that addressed [CVE-2020-14728](https://nvd.nist.gov/vuln/detail/CVE-2020-14728), which may be related to this IDOR.

Outside of this hint, the root cause of this issue is unknown at the time of this writing. It may be as straightforward as updating the local NetSuite instance, or there may be more local configuration needed to ensure that sales order receipts require proper authentication in order to read them.

**Post-authentication considerations**

Note that becoming an authenticated user is trivial for the Primary Arms website. New users are invited to create an account, and while a validly formatted email address is required, it is not authenticated. In the example gathered here, the simulated attacker, FakeTod, has the nonexistent email address of todb@example.com. Therefore, there is no practical difference between an unauthenticated user and an authenticated user for the purpose of exploitation.

**Impact**

By exploiting this vulnerability, an attacker can learn the PII of likely firearms enthusiasts. However, exploiting this vulnerability at a reasonable scale may prove somewhat challenging.

**Possible valid IDOR values**

It is currently unknown how the salesorder values are generated, as Rapid7 has conducted very limited testing in order to merely validate the existence of the IDOR issue. We're left with two possibilities.

It is the likely case that the salesorder values are sequential, start at a fixed point in the 8-digit space, and increment with every new transaction in a predictable way. If this is the case, exhausting the possible space of valid IDOR values is fairly trivial — only a few seconds to automate the discovery of newly created sales order records, and a few minutes to gather all past records. While limited testing indicates salesorder values are sequential, there are gaps in the sequence, likely due to abandoned and partial orders. We have not fully explored the attack surface of this issue out of an abundance of caution and restraint.

In the worst case (for the attacker), the numbers may be purely random out of a space of 100 million possibles. This seems unlikely according to Rapid7's limited testing. If this is the case, however, exhausting the entire space for all records would take about two years, assuming an average of 100 queries per second (this probing would be noticeable by the website operators assuming normal website instrumentation).

The truth of the salesorder value generation is probably somewhere closer to the former than the latter, given past experience with similar bugs of this nature, which leads us to this disclosure in the interest of public safety, documented in the next section.

**Possible attacks**

We can imagine a few scenarios where attackers might find this collection of PII useful. The most obvious attack would be a follow-on phishing attack, identity theft, or other confidence scam, since PII is often useful in executing successful social engineering attacks. An attacker could pose as Primary Arms, another related organization, or the customer and be very convincing in such identity (to a third-party) when armed with the name, address, phone number, last four digits of a credit card, and recent purchase history.

Additionally, typical Primary Arms customers are self-identified firearms owners and enthusiasts. A recent data breach in June of 2022 involving [California Conceal Carry License](https://www.jdsupra.com/legalnews/california-department-of-justice-3366057/) holders caused a stir among firearms enthusiasts, [who worry](https://thereload.com/new-california-ag-website-leaks-massive-trove-of-gun-owner-private-information) that breach would lead to "increase the risk criminals will target their homes for burglaries."

Indeed, if it is possible to see recent transactions (again, depending on how salesorder values are generated), especially those involving FFL holders, it may be possible for criminals to intercept firearms and firearms accessories in transit by targeting specific delivery addresses.

Finally, there is the potential that domestic terrorist organizations and [foreign intelligence operations](https://www.opensecrets.org/news/2021/10/russia-pouring-millions-into-russian-foreign-influence-kremlin-propaganda-targeting-the-us/) could use this highly specialized PII in recruiting, disinformation, and propaganda efforts.

**Remediation**

As mentioned above, it would appear that only Primary Arms is in a position to address this issue. We suspect this issue may be resolved by using a more current release of NetSuite SuiteCommerce. A similar e-commerce site, using similar technology but with a more updated version of SuiteCommerce, appears to not be subject to this specific attack technique, so it's unlikely this is a novel vulnerability in the underlying web technology stack.

Customers affected by this issue are encouraged to try to contact Primary Arms, either by email to [info@primaryarms.com](mailto:info@primaryarms.com), or by calling customer service at +1 713.344.9600.

**Disclosure timeline**

*Update:*Since the publication of this report, Primary Arms reached out to Rapid7 to confirm receipt of the original report and implemented a fix resolving the IDOR issue.