The BSA Examiner©

A Quarterly Publication from Wayne Barnett Software
Volume 95, 3rd Quarter 2024

The BSA Examiner is a quarterly newsletter published by Wayne Barnett Software. If you have a question to ask or a story to tell (we promise anonymity), please call us at 469-464-1902.

Case #1—Brilliance appreciated!

My wife was expecting a package from Damon and Draper (a woman's clothing retailer). A few days after the package was scheduled to arrive, she received an email stating that a delivery error resulted in the package being sent to the Postal Service Delivery Resolution Center (PSDRC). The email appeared to come from DHL Express. We checked the tracking number, and the USPS website confirmed that the package was at the PSDRC.

Why are we writing about an errant package delivery, you ask? Let us please explain.

1. It's likely the package was correctly delivered, on the scheduled day. However, before we could retrieve the package from our mailbox someone took it.

2. The person who took the package didn't want the contents. In fact, the thief likely dropped the package in a mail collection box later that same day.

3. So, why was the package stolen if the contents weren't taken? It's because the thief wanted to send my wife an email, where she could see that her package was being held at the PSDRC and would be delivered in 7-10 days.

    a) However, the email explained that expedited delivery could be had for a fee of $0.58. A link to pay the fee was in the email.

    Note: some people may be wondering how the thief got my wife's email address. Well ma'am and sir, if I have your name and street address, I can legally buy a list of your commonly used email addresses. Marketing firms will sell you 2,000 email addresses, based on someone's name and street address, for $200 (or $0.10 per person).

Back to our story: needless to say, we were dubious of the email that appeared to have come from DHL Express.

4. Yes, it did correctly show that our expected package was at the PSDRC.

5. And the URL for the optional fee-payment web site began with HTTPS (which means it had a legitimate security certificate, as required by Microsoft and Google).

6. But the whole thing didn't feel right.

    a) We had no way of contacting USPS to ask if DHL delivers misrouted packages.

    b) Also, $0.58 seemed like a low amount for a service requiring this much work.

    c) So, we used the Internet to see what we could learn about the optional payment web site.

i. Of the five Web Security Services (WSS) we checked, four said the URL had a good reputation.

ii. The fifth WSS said the same thing, but it also noted that the URL had only been in existence for four (4) days.

iii. At this point, we checked to see where the web site was located (which you can do at https://check-host.net). The site was hosted on a server in Hong Kong.

So, to surmise, a web site that was four days old and located in a communist country wanted us to enter our credit card information to pay a fee of $0.58, so that my wife could get prompt delivery of her new clothes.

7. Now, most people would stop at this point—but not us. We wanted to see what happened next, so we entered our credit card information.

    a) The site quickly came back with a message saying, "We're sorry, Citibank is currently off-line. Please enter another card (may we suggest American Express)."

    b) We don't have an AmEx card, so we tried to pay the $0.58 bill with our Discover Card—only to learn that Discover was also off-line (what are the odds?)

8. We immediately closed the website. My wife called Discover, and I called Citi.

9. Both Citi and Discover informed us that a request had already been made to link our cards to a newly established Apple Pay account. The requests were denied.

    a) It took less than two minutes for the hackers to try and link our credit cards to their new Apple Pay account.

10. We hate hackers, but we were impressed with the sophistication of this scheme. But having said that, we were more impressed with the brilliance of the security staff at Citi and Discover. Great job folks!

Bottom line: if your bank issues credit cards, we recommend you assess how your servicer handles a situation like this. Also, if your bank's web site has a link to a Web Security Service (and many do), we recommend you evaluate it for reliability. If age and server location don't factor into a web site's rating, we recommend finding a new WSS.

Case #2— Same outcome, different victims.

A few years back, commercial businesses were victimized by the "thousand-cut fraud".

1. This crime involved an established company (often a small business providing pallets, cleaning supplies, or other low-cost products) being bought by criminals, and the criminals subsequently stealing large sums from the company's customers.

    a) The thieves focused on buying seller-financed businesses that had around 100 customers.

    b) The thefts were committed with a series of small ACH transactions. The transactions were typically in the range of $300 - $500 each.

c) The goal of the thieves was to steal $5,000 - $15,000 from each victim, and then disappear. They were highly successful.

d) A few of the thieves were caught and prosecuted. But this theft continued mostly unabated for three years.

i. Since the thefts were from commercial customers, Reg E did not apply. Rather, NACHA rules governed who took the losses.

ii. In most instances, the losses were borne by the receiving banks. The reason for this: NACHA rules imply that banks are supposed to look for and stop thefts like this.

iii. It was software like ours and Verafin's that ultimately enabled bankers to fight back and make this type of crime a nonissue.

Well ladies and gentlemen, the thousand-cut fraud is back—but this time the thieves are targeting consumers and using fraudulent checks.

1. Young people working in retail are being encouraged via a Tik Tok video to take pictures of checks accepted at work, and to upload the pictures to a web site.

2. The maker of the Tik Tok video claims to sponsor a weekly random drawing. If the check you send is selected, the account owner and the person who sent the check both win $1,000.

3. We're sure our readers aren't surprised to learn this is a scam.

   a) The people receiving the images are using them to create counterfeit blank checks; all writing on the check is removed (including the signature).

   b) The counterfeits are indistinguishable from the original checks—except that the check numbers are incremented. (This attention to detail even surprised us.)

   c) The thieves are using the checks to buy things that are easily resold on eBay. The amount of a typical fraudulent check is $400 - $700.

   d) The thieves steal from each victim just once a day. The low amounts combined with the low frequency of the transactions make it much harder to detect.

   e) Even low amounts quickly add up. Federal law enforcement officials told us the thefts usually last two weeks. The average amount stolen is around $5,000.

4. How common is this theft? In a word: very. In fact, some national retailers have announced plans to stop taking personal checks. (One such retailer is Hobby Lobby.)

Bottom line: banks typically aren't aware of these types of thefts until the customer complains or the account is overdrawn. Software like our Suspicious Activity Monitor system can give you a big advantage in combating these thefts.

We are Wayne Barnett Software. We're not a big company, but our products compare nicely with Verafin, Abrigo and the other software giants (none of whom will care about you as much as we do!) You can contact us at https://www.barnettsoftware.com/contact-us/, 469-464-1902, or wbarnett@barnettsoftware.com. Thanks for reading our newsletter.