SECURITAS

2nd QUARTER 2016

While you may not see the stories on major news networks, smartphone theft is big business and you would be surprised to learn that in 2013, 3.1 million smartphones were reported stolen in the United States[1]. It may also come as a surprise that nationally, just under a third of all robberies involve a smartphone of some kind.[2]

A stolen smartphone (or tablet) represents a win-win for the thief because they have your device and in many cases, they get the information inside that device. Identity theft (and fraud) often begins from within a stolen device. Remember that ID theft is merely the stealing of your information. ID *fraud* occurs when the would-be thief uses your information for financial gain (loans, lines of credit, using your credit card to purchase groceries or gas).

So, ask yourself, "What if my iPhone or iPad (or computer) was stolen? Would I know what to do? Could I track and erase the data on my device?" In answering these questions, the first suggestion would be to *learn* about your technology and any such capabilities. Knowledge of how you can protect, track and erase your device is an essential first step. Having this knowledge will give you confidence when creating a plan in case your device is lost or stolen. In this article, you will find two scenarios where having a plan is crucial.

- What to do when a personal device (computer/tablet/smartphone) has been stolen.
- What to do when someone has used my identity to make a purchase or secure a loan.
    - Stolen card numbers are a more likely event and represent an easier mark for the thief. Stealing enough information about you to secure a loan is a different problem altogether.

Another suggestion would be to prepare yourself for a potentially daunting exercise in perseverance and patience. Living through either scenario is not going to be fun – but executing a well-prepared plan will make the experience much more manageable.

Scenario #1 – Your tablet/phone was lost or stolen while on vacation (or from any location). We will use an Apple product as an example.

1. **Don't panic** – I say that because I assume you have already placed a passcode on the device. This is the FIRST line in the defense of your identity/privacy. If your iPad/iPhone or other tablet has no barrier between it and the general public – everything is fair game to the lucky thief.
2. **Make a Call** – If you suspect theft, notify the local authorities and try to retrace your steps in an effort to identify where the device went missing. Also, call your investment advisor, banker, CPA, etc to notify them of the potential theft. Many phishing emails originate from a client's stolen device.

[1] http://www.wired.com/2014/12/where-stolen-smart-phones-go/
[2] Ibid

3. **Track your device** – Apple gives you the ability to locate your devices (iPads, Macs, iPhones) via the www.icloud.com. I encourage you to learn more about how Apple and Android help protect you and the information on your devices.
4. **Change your passwords** – Strongly consider changing *any* password associated with email located on your device. Other password changes could involve banking/credit card apps and shopping apps as well. Definitely change the account password for your AppleID (or Google Play if applicable).
5. **Notify your banks and credit card companies –** If you had your bank account(s) and credit card data integrated into your phone through their apps, notify them immediately and request that an alert be placed on your account. They may offer other helpful suggestions as well.

Scenario #2 – What to do when someone has used my identity to make a purchase or secure a loan.

There are fantastic resources that I would like for you to consider when thinking about your response to personal identity theft. The first link below is a more concise approach titled, "What To Do Right Away." You might want to print this out and have it ready just in case…

https://bulkorder.ftc.gov/system/files/publications/pdf-0204_identitytheftwhat_to_do_right_away_0.pdf

The second link is "Taking Charge: What To Do When Your Identity is Stolen" and will help you build a personal recovery plan.

https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf

I encourage you to spend some time in these documents and work through them to build a greater awareness of where you have the most exposure.

Identity thieves and fraudsters gain the most from victims who are not prepared. A victim who has a plan, knows their technology and who to call can mitigate much of the risk that comes from a stolen device. Being able to quickly respond to these events will save you time, money and hopefully some sanity.

A premium is often placed on investing in financial markets, our careers and healthy lifestyles. While these are worthy endeavors, we live in a world that requires more diligence in protecting and caring for our privacy and identity. The former usually takes time to realize a return, if any. I believe the latter will most certainly benefit you not only in the short run, but in the long run as well.

Written by Jon Atchison
Information Security Coordinator for Welch Hornsby, Inc.