Black Friday, Small Business Saturday and Cyber Monday: Fraud Prevention Awareness for Consumers

By: Jim Mottola
Director of Forensic Investigations
Risk Mitigation Services, Sobel & Co.

This is the time of year that most of us will be checking off our shopping lists as we are standing in line at the mall, a boutique or sitting in front of a computer screen trying to take advantage of the greatest deals of the season. That being said, before leaving the house or clicking a mouse every consumer should also be thinking about protecting themselves from Identity Theft. To that, I have my own list to increase consumer awareness to fraud, wherever and whenever they shop, in both the physical and digital world.

Identity Theft

An incident affecting the genuine information on a credit report can itself can be terribly inconvenient, even an arduous process, for a consumer to repair. The likelihood of this occurring may be a lot less than it was a number of years ago, due to the fact that Identity Theft as a crime has been pushed to the forefront by financial institutions and credit reporting agencies, however, the impact is still very high. According to IdentityHawk.com, the Federal Trade Commission recently estimated that recovering from identity theft could take an average of six months and 200 hours of work.

The vulnerability lies within the plethora of personal information exposed as part of the information age and as a result of countless criminal hacker attacks and theft of data. For the individual, the loss and theft information by improperly discarded paper statements can be just one method of compromise. Careless online behavior compounded by social engineering scams perpetrated by fraudsters represent and an additional area of concern.

Things to Do

- ✓ Obtain a recent credit report in order to determine your baseline or the current state of financial consumer credit. I actually encourage everyone to do this, at least once a year, in order to take inventory of unwanted or unused lines of credit. Cancelling accounts which are no longer active or less frequently used may also save you from fees or late charges.
- ✓ Enabling credit monitoring services such as Transunion, Experian and Equifax will allow you to get alerted from all three companies or lock a report. Also, a review of these statement will allow someone else to monitor inquiries and reveal fraud. Unlike credit card companies these features are not included as a free service.

- ✓ Properly shred and discard any paper statements with your personally identifiable information (PII).
- ✓ Report lost or stolen cards or documents immediately. A "freeze" can be put on an account.

Credit Cards

The exposure for card holders is moderate to high; however, the residual effects of having your card compromised usually amounts to an inconvenience. Banks, retail and E-Commerce sites are the most vulnerable and are very likely to be the point of compromise. For the consumer lost or stolen cards, discarded paper statements and lack of responsible online behavior can also lead to the theft of accounts. However, the good news is that banks have significantly improved their data analytics in order to quickly respond to fraud and thus rarely affecting the consumer in the long term. Again, the greater concern here is that a criminal may have access to your personal and financial information which is a much bigger problem. If you are a victim of fraud, contact the aforementioned credit reporting companies, you should be able to get a credit report for free. Also, ask your bank to provide free credit monitoring.

Things to Do:

- ✓ Reduce exposure by lowering available credit amount, where practical. Increase as needed for out of pattern or high dollar purchases, such as overseas travel.
- ✓ Properly shred and discard any paper statements.
- ✓ Do not use a debit card as a credit card. It is directly linked to a bank account and if compromised, it takes much longer to resolve and could result in a significant amount of funds stolen from an account. This is the worst case scenario for credit and debit cards. Use it solely to conduct banking transactions.
- ✓ Report lost or stolen cards immediately. A hold can be put on a card if you are unsure. You can also check the last purchase.

Bank and Brokerage Accounts

The exposure for bank and brokerage accounts is low to moderate, as most institutions do a fairly good job at protecting clients. However, this is another fraud scheme where the resulting recovery of funds can be arduous and time-consuming. Criminal hackers have been targeted financial institution with best in class cracking tools and malware, so the threat is real and persistent. Again, for consumers protect yourself by safeguarding your account information to include the password in both physical and digital environments. The good news here is that financial Institutions are under intense regulatory and reporting requirements. Consequently, their oversight is generally very good. The bigger the institution, the safer your money is likely to be. Or the more likely you are to be notified of a theft and/or be reimbursed. However, if you are at fault, it could be an entirely different situation.

Things to Do

- ✓ Credit monitoring and review often your reports and statements.
- ✓ Properly shred and discard any paper statements with your personally identifiable information (PII).
- ✓ Report lost or stolen cards or documents immediately. A "freeze" can be put on your account.
- ✓ I would also inquire as to specific notification procedures an institution has in place to validate large withdrawals and trades, real-time.

Online Activity

Simply put the exposure for the consumer here is very high, especially when you consider that criminal hackers are excellent at using behavioral manipulation or social engineering to leverage bits of information to compromise consumer data. The good news is that many software security applications are available for the user, and online behavior can be modified to limit the exposure. I am also a big fan of the offline backup of data to a local hard drive, cloud storage and yes, a few critical paper documents locked away in a filing cabinet, just in case.

What to Do

- ✓ Password Management: Change periodically; create unique and hard to guess passwords for each account; do not store in clear text on PC. Many solutions exist such as the Last Pass.
- ✓ Install Antivirus Software, such as Norton, and update frequently. It's better than nothing.
- ✓ Update the operating system as needed, Apple, Android and Microsoft Updates for all devices.
- ✓ Don't open suspicious emails, from known or unknown senders.
- ✓ Don't store critical documents on the hard drive such as tax documents. Google Drive, DropBox Apple has simple and relatively secure data storage solutions.
- ✓ Secure on-line account passwords by not using autosave: enter each time you log on and don't save them in an unencrypted file such as word document named passwords.

On-Line Presence

Google yourself, it is fun for about 5 seconds, until you realize how much of your personal data is actually exposed online. Often our own company's website is a great resource for the fraudsters. Start with www.Spokeo.com, then www.123peoplesearch.com, enough said. For most of us, it will be very time consuming and expensive to remove ourselves from these databases. There are services that can perform this service, and if you are interested I can point you in the right direction. Otherwise, review your social media pages to limit the amount of information you provide for free. Unfortunately, every time we agree to terms and agreements for another online service, a business is aggregating our data for sale, because it is valuable.

Keep Shopping: One Step at a Time

To be always secure or to protect our information from never being compromised is now impossible. However, we can lower the frequency and impact by taking steps to do mitigate the inevitable through security awareness and our own actions. By taking the time to approach this situation through a defense-in-depth, or a layered approach we can achieve a better level of security and although it may be somewhat inconvenient, it should greatly improve your chances of protecting your information. Remember, while most fraudsters will specifically target business or organization, individual consumers can usually get tangled up in the web of a larger scheme, as we have often witnessed. So buyers beware, don't let anyone ruin your day, not even the Grinch.