FORT VANCOUVER
INVESTMENT MANAGEMENT

You, Your Advisor and Schwab: Partners in Safeguarding Your Financial Privacy and Security

A Fort Vancouver Investment Management Special Report
March 2013

As technology delivers countless improvements and opportunities for better managing our wealth, it also delivers new vulnerabilities, further exacerbating the challenges involved in protecting our personal information. As is usually the case in protecting your security, the most effective strategy is a multi-pronged attack from a unified force. You and your financial team should work in concert to expose vulnerabilities and shore up breaches. For Fort Vancouver Investment Management clients, this involves a partnership among you, us and your asset custodian, Charles Schwab.

Here we present an overview of distinct and combined roles we each play in this battle immemorial against threats to your financial privacy and security.

FORT VANCOUVER INVESTMENT MANAGEMENT'S ROLE

There are several ways we, as your investment advisor, help safeguard your financial security as well as your individual privacy.

Maintaining Your Privacy

For starters, we maintain and share our privacy policy with you annually. It is both our requirement and privilege to keep you apprised on how we handle your personal information. We also are happy to share our privacy policies with you upon request at any time. We've attached our current policy with you as Appendix A to this report.

We also must be prepared to present our privacy procedures at any time to our state regulator. We must further be ever-prepared to demonstrate we are enacting our policies should a regulator wish to conduct an on-site audit of our offices — announced or as a surprise visit.

Asset Custody

In addition, among the most significant ways we as your investment advisor help safeguard your financial security comes from a source you may not immediately recognize as related to the issue. It has to do with who your financial custodian is.

"Custodian" is the industry term for who is holding your money when it's not stuck under your mattress. In your relationship with us, **Schwab Institutional** is your custodian for your assets that we manage. We are **not** a custodian; we are your advisor. We do dispense investment advice and then help you implement it by overseeing the transactions going into, coming out of and remaining within your Schwab accounts. But, with the exception of the quarterly advisor fees you pay us in exchange for the services we provide,[1] you will never write a check made out to us, nor hand us cash to invest on your behalf. Likewise, we don't make payments from us to you. All monetary transactions are between you and your fully independent custodian, Schwab.

If you think arm's length custody isn't important to preventing breaches in your security, we need bring up only one name to make our point: Bernie Madoff. Among the key tricks Madoff used to perpetuate his infamous Ponzi scheme was serving as both advisor and custodian to his clients' assets. The dual roles made it easier for him to hide his trail of misdeeds in all the reports his clients were receiving. In the case of Madoff, the numbers did indeed lie.

The concern has not disappeared post-Madoff. In March 2013, the financial trade journal *InvestmentNews* reported that the Securities and

[1] Your quarterly advisor fees are typically automatically paid to us from your Schwab accounts, and then fully and transparently reported to you in your Schwab statements as well as within our separate reports to you.

Exchange Commission (SEC) has been cracking down on custodial issues in its recent advisor audits. "Because the safeguarding of assets is central to investor protection, it is critical that investment advisers follow our rules when they maintain custody of their clients' funds," SEC Chairman Elisse Walter said.[2]

Ensuring SEC-regulated, arm's length custody of your assets is why you receive overall portfolio performance reports from us, while you receive your individual trading and account status information directly and separately from Schwab. This not only helps you remain apprised of how your investment activities are doing, it offers you a double-safe system for verifying that your assets are being employed as intended. Thanks to the convenience of online technology, you can access your Schwab accounts at any time and confirm that the information we're sharing with you matches the transactions, account balances and similar information reflected in Schwab's reports. In our partnership to protect your financial security, this is among your responsibilities – for your assets we are managing, as well as for any you may be holding among other relationships.

SCHWAB INSTITUTIONAL'S ROLE

Beyond custody issues described above, Schwab takes its commitment to safeguarding your information very seriously.

Schwab Privacy and Employee Policies

This starts with Schwab's employees and privacy policies. While it is necessary for them to gather private information to open accounts, they restrict who has access to your private information within their company and train their employees regularly on privacy and security. They *do not* sell your private information to other companies. At times, Schwab does share your information with other Schwab affiliates in order to provide you with more comprehensive service. There are also a few occasions when they share information with outside companies. These instances are limited and may arise when processing a transaction for your account, when using another company to provide a service for them, such as an outside printing company, or when disclosure is required or permitted under law (such as to perform credit/authentication checks, resolve consumer disputes, etc.). If you would prefer for Schwab to limit information shared, you may contact them at 877.812.1817 to discuss your options.

Online Security

SchwabSafe is Schwab's collection of online security measures created to keep your private and financial information safe. Some of the highlights are listed below. You may visit the SchwabSafe portion of Schwab's website for further details:

- To protect your account from unauthorized access, Schwab has implemented multiple layers and factors beyond the login ID and password used when accessing your account. If unauthorized activity is suspected, Schwab will ask for additional verification before permitting account access.
- Schwab also uses advanced encryption technology which allows safer communication between Schwab and their clients. The highest levels of secure certificates are used. Before logging in, look for the green web address bar and check to make sure that the web address begins with "https" versus "http." The "s" on the end stands for "secure" and signals the browser to use an added layer of encryption.
- A timeout feature has also been added. This feature will log you out of your account after a certain period of inactivity. This helps stop others from accessing your account if you forget to logout.

[2] Mark Schoeff Jr., "SEC warns investors that advisers could be mishandling assets," *InvestmentNews*, March 4, 2013.

Additional Protection

Schwab has also created the Schwab Security Guarantee which covers 100 percent of any losses due to unauthorized activity. For this guarantee to be valid, you must report8 any issues to Schwab immediately, and Schwab must be able to verify that the unauthorized activity was not due to client negligence, such as if you inappropriately shared your private information. For further details, you can visit Schwab's Security Guarantee page.

YOUR ROLE

As touched on above, it is vital that you take an active role in protecting your private information. Following are a few tips and resources to get you started.

Safety Begins at Home

In addition to keeping an eye on your safe and secure account information, many steps to financial security and privacy begin at home, especially your home (and, these days, mobile) devices.

- Keep all software and browsers software updated.
- Install and regularly update anti-virus and anti-spyware software on all of your devices.
- Use personal firewalls and never turn them off.
- Do not choose any auto login options for any websites or apps that you use.
- Keep your login ID and passwords private at all times. From time to time, change your passwords. Also, avoid using the same password for everything, as criminals have been known to obtain user names and passwords from less secure websites, and then try using them on more secure and mission-critical websites, such as your bank's. For tips on creating effective passwords, visit Microsoft's Safety and Security Center:

- Whenever possible, avoid making financial transactions or logging into secure websites, such as Schwab or other banking websites, from public computers or public Wi-Fi hot spots. If you can't avoid it, never save your login information and always click "log out" when you're done. Don't leave the computer unattended while logged in, or with any sensitive information on the screen, erase your tracks (delete browser history if you're able), and watch for people potentially looking over your shoulder – physically or virtually – to obtain your private information.
- Treat your cell phone or other devices like your children: Don't let them talk to strangers. Do not allow your cell phone or other devices to automatically connect to non-preferred networks; the connection may be an undesirable one.
- For your Schwab account, order a free security token to use as an additional layer of security when logging in. This token is a small device that generates a six-digit number for you to enter when logging on to the Schwab website. Basically, producing a new password each time you log in. You may call Schwab at 800.435.4000 to request this device.

E-Mail Fraud and Phishing

E-mail fraud and phishing are additional threats to guard against in your identity theft battles.

Phishing is a form of identity theft that attempts to mislead you into providing personal or financial information — including account numbers, passwords and Social Security numbers — through phone calls, e-mail or fraudulent websites. The following are signs of a phishing scam:

- An e-mail request for immediate action on an account-related matter, usually with an "urgent" tone to the e-mail.
- Spelling errors and bad grammar. With multiple editors, professional organizations typically will not allow a mass e-mail to include errors.

- An unsolicited e-mail with an attachment or recommended website hyperlink sent from someone claiming to be a legitimate company. Do not open the attachment nor click on the link!
- A pop-up window appears with a request for your personal information and claims to be a real company's website.

If you think you've run into phishing scams, whether by e-mail, phone or a fraudulent website:

- Never share your personal information.
- Do not click on links within the e-mail as they may install malware on your computer.
- Do not open any attachments as they may contain a virus that will infect your computer.
- If you receive a call that you suspect is a phishing scam, take down the caller's information and notify your local police department.

To learn more about phishing scams, you can visit www.antiphishing.org. Or another handy resource is http://www.consumer.gov/section/scams-and-identity-theft. If you suspect you have received a fraudulent e-mail from Charles Schwab or one of its subsidiaries, you may forward the suspected e-mail to phishingawarenessteam@schwab.com or call 800.515-2157. Their team will research the issue and try to stop it.

If you are a victim of identity theft, the Federal Trade Commission (FTC) recommends the following steps:

- Contact your financial institutions to let them know.
- Contact the fraud department at the three major credit bureaus.
- Request and carefully review copies of all credit reports.
- Contact the fraud department of creditors to dispute any unauthorized charges.
- Call your local police department and ask to file a report.
- File a complaint with the Federal Trade Commission (FTC) which handles complaints of victims of identity theft. You may contact them by phone at 877.ID.THEFT or via their online complaint form on their website ftc.gov/complaint.

The FTC's website also provides a good resource for initially informing yourself about identity theft, as well as remaining abreast of any new information on that front:

CONCLUSION

Identity theft and financial security breaches are as ancient as mankind itself. With the advent of latest mobile technology and the increasing freedoms it brings, come increasingly clever scam artists seeking to topple your security. Basic geometry informs us that the strongest base is formed by a triangle. Two legs to your safe and secure financial protection include us as your advisor and Charles Schwab as your custodian. The vital third leg is YOU. We encourage you to take an active part in defending your assets. We also encourage you to turn to us as your partner, letting us know whenever you have questions or you feel there may be ways we can help you further protect your financial security.

FORT VANCOUVER
INVESTMENT MANAGEMENT

Appendix A
Privacy Statement

Fort Vancouver Investment Management, LLC, an independent registered investment advisor firm, is committed to safeguarding the confidential information of its potential, current and former clients. We value our relationship with you and understand that the information you have entrusted to us is private. Our goal is to be worthy of that trust. Our privacy policy with respect to nonpublic personal information about you is stated below.

1. **We do collect personal information in order to open and administer your accounts with us and to provide you with accurate and pertinent advice. We hold all personal information provided to us in the strictest confidence.**

    - We collect personal financial and tax information that you provide to us.
    - We collect account opening information that includes name, birth date, Social Security number, street and e-mail addresses, telephone numbers and employment information.

2. **We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law. Your account opening information is shared with the custodian/s from whom you receive account statements.**

3. **We protect the security, integrity and confidentiality of your personal information.**

    - We maintain a secure office and computer environment.
    - All employees are trained and required to safeguard your information.

4. **We do not sell your personal information to anyone**.

5. **We will provide notice of changes in our information sharing practices. If, at any time in the future, it is necessary to disclose any of your personal information in a way that is inconsistent with this policy, we will give you advance notice of the proposed change so you will have the opportunity to opt out of such disclosure.**

    - If you identify any inaccuracy in your personal information, please contact us so we may promptly update our records.

If you have any questions about this policy, please contact us via the office information on this letterhead.

1607 Officers Row, Vancouver, WA 98661
(360) 823-0477 (Vancouver) | (503) 210-2219 (Portland) | (877) 623-0477 (Toll Free)
www.fortvancouverim.com