NORTHWEST FINANCIAL ADVISORS
INFORMATION SECURITY DISCLOSURE

As your lifetime financial partner, there is nothing more important to us than your financial well-being. Just as we prudently and cautiously care for your assets, we take every precaution to ensure that your personal and private information is protected from unauthorized access and harm. As a wholly owned subsidiary of Northwest Federal Credit Union (NWFCU), we adhere to NWFCU's security policies and procedures. Since we are also a registered investment advisor (RIA) firm and our clients' assets are custodied at LPL Financial (LPL), we must also adhere to LPL's information security policies and procedures, as well as all federal and state regulations.

What is Cybersecurity?

a.) Cybersecurity is the combination of technology, processes and practices which are designed to protect networks, computers, programs and private and proprietary data from cyberattack damage or unauthorized access. As an RIA firm, Northwest Financial Advisors (NWFA) must ensure that we have proper cybersecurity protocols in place. Your personal information and account data are protected by NWFCU, LPL and our own security measures. You may visit LPL's website to learn more about LPL's policies regarding Consumer Privacy, Online Privacy and Identity Theft Prevention. Also, NWFA undergoes periodic audits by federal and state regulators, as well as LPL, which include reviews of all cybersecurity processes and practices.

How is my electronic information and data being protected from malicious outside sources?

a) We employ a Layered Security model to protect our network and physical resources from malicious outside threats and unauthorized users from accessing client data. Layered security is the practice of combining multiple mitigating security controls to protect resources and data, and to slow, block, delay or hinder a threat until it can be completely neutralized. Understanding there is no "silver bullet," these different layers of defense cover all known vulnerabilities and will continue to grow as new threats tax current defenses.

How is my information and data physically protected from malicious activity?

a) New hire onboarding includes an LPL Financial regulatory background check. In addition, regular background checks through LPL are required for all personnel who may come into contact with Personally Identifiable Information (PII).

b) Access to our physical office location where PII is stored or used is restricted to authorized persons. We secure and control access to dedicated computers, printers, copiers and fax machines. This includes housing equipment behind locked doors and controlled access security systems. NWFA does not share office space with credit union employees.

c) Discarding of documents that contain PII or confidential information is done by collecting documents in special containers and either burning or pulping them.

d) Terminated personnel are required to immediately surrender all employment related IDs, badges, business cards, computer equipment and other items which permit physical and electronic access. Our in-house IT support team disables all computer/email access immediately upon employee termination.

How can you ensure that if my Personally Identifiable Information (PII) is compromised, no one could trade my account or move my money?

a) Trade orders from clients may only be done via a phone call, which allows us to directly authenticate the caller. Knowing our customers is a crucial part of our business.

b) If your PII is compromised and a call is made directly with LPL to liquidate your account, money movement would require a signed form to be completed and the transaction confirmed by your NWFA financial advisor (advisor of record). If previous instructions are already on file such as an ACH set up, those procedures would need to be followed unless a new form is completed, signed by you and acknowledged by your advisor. If a check is requested to be sent to an alternate address, a form is required to be completed, and your advisor would need to validate the account holder. If a third-party wire is attempted, again, this would require a signed form by both the account holder and the advisor. All attempts must pass through several required layers of authentication.

What if my email is hacked and someone attempts to contact NWFA by email to access my account?

a) It is NWFA's policy and industry standard that all trade and money movement requests be done so via a phone call to confirm the identity of the account holder. No trade or money movement will be completed without us directly authenticating (validating) the account holder. Although rare, we have seen and thwarted these types of attempts. In such cases, we notify the account holder in question, as well as LPL, as they are required to alert their Financial Intelligence Unit of such fraud. LPL may also place a restriction on the account if deemed necessary.

What about portable devices such as laptops, tablets and cell phones? Can my personal information or data be compromised through those devices?

a) Every advisor or staff member utilizing mobile devices for business must adhere to policies set in place to ensure client data safety. Our IT team confirms that whole-disk encryption is placed on every laptop, password and lock-out policies are systematically generated, cell phones are only accessed via entry of a password and multiple unauthorized access attempts would erase the device.

Unfortunately, in today's environment, we are all vulnerable to malicious cyberattacks. Some of the seemingly safest companies and organizations have had data breaches. No system can be 100 percent impregnable against trained and resourceful hackers, but we promise to always:

- Put cybersecurity policies and procedures in place with the distinct and clear purpose of fully protecting our clients' personal and account information from exposure and harm
- Train our personnel to adhere to all practices and procedures
- Regularly test our practices and procedures through mock penetration tests and vulnerability scans (both internally and externally)
- Modify our practices and procedures when necessary
- Stay abreast of changing federal and state regulations, as well as NWFCU and LPL Financial policies and practices
- Expeditiously and diligently follow our practices and procedures in case of suspicion of or actual attempts at fraud
- Provide our clients with access to our firm's information security policies and practices at all times
- Notify our clients of any suspicious or actual attempt at fraud in an urgent manner

If you have additional questions about our information security procedures, please contact Nicole Davis, NWFA's chief compliance officer, at ndavis@nwfllc.com.