S&L Fraud Prevention Fireside Chat Summary & Notes

8/4/26

Speakers:

Dalal Salomon, Founding Partner, Salomon & Ludwin
Page Adlington, Senior Manager, Business Consulting and Education, Charles Schwab

The following key areas of concern and education were discussed:

- **Protecting email accounts** from compromise, which was identified as the leading source of financial fraud
- **Credit monitoring and credit freezes** as effective tools to prevent unauthorized credit activity
- **Password management best practices**, including the use of paid password managers and avoiding free versions
- **Multi-factor authentication** preferences (phone-based codes over email-based codes)
- **Wire transfer and real estate transaction fraud**, illustrated by a real-world $4 million fraud case involving a compromised email chain and a substituted title company account number
- **Schwab's fraud prevention protocols**, including verbal verification requirements for money movements and the role of trusted contacts

Summary

Topic	Impact	Summary
Email Security & Fraud Prevention	Asset protection; preservation of account integrity	Email compromise identified as the primary vector for financial fraud; fraudsters may reside in an account for months before acting
Credit Freezes & Monitoring	Identity protection; prevention of unauthorized credit activity	Freezing credit at all three bureaus is highly effective; services such as LifeLock can bundle monitoring, freezing, and VPN

Topic	Impact	Summary
Password Management	Account security; reducing unauthorized access risk	Paid password managers recommended; Apple Keychain acceptable for single-device use; free versions discouraged
Multi-Factor Authentication	Account access security	Phone-based codes preferred over email-based codes; authenticator apps and text-based codes considered equally effective
Wire Transfer & Real Estate Fraud	Protection of large financial transactions	Verbal verification of account numbers with title company or closing attorney is essential before moving funds
Schwab Account Safeguards	Client account protection	Schwab requires verbal verification for money movements; trusted contacts can be designated for additional oversight

Detailed Notes

Email Security & Fraud Prevention
Email compromise was identified as the leading cause of financial fraud — described by Page Adlington as "cyber public enemy number one." Fraudsters can gain access to an email account and remain undetected for months or even up to a year, monitoring transactions, identifying parties involved (attorneys, title companies, CPAs), and waiting for the right moment to act. Nearly all successful fraud cases at Schwab can be traced back to a compromised email account. Key protective measures discussed included: using strong, unique passwords for each account; investing in paid antivirus software; never sending confidential documents (tax statements, account statements, applications, or any identifying information) via email; and using secure portals for sensitive communications. Attendees were advised to change passwords immediately if they notice unusual activity or receive reports of suspicious emails sent from their account.

Dalal shared that Salomon & Ludwin operates on constant high alert to protect client information and accounts. Director of Operations Willene Bellamy and the operations team attend cybersecurity workshops and training regularly. Any request from the operations team for additional verification is a deliberate protective measure, not an inconvenience.

- **Impact on Lifetime Portfolio Value -** A compromised email account can expose clients to significant financial loss through unauthorized money movements. Preventing email compromise is a direct safeguard for portfolio assets.
- **Impact on Projected Cash Flow -** Fraudulent wire transfers or unauthorized transactions initiated through a compromised email can result in immediate, material cash flow disruption.
- **Impact on Tax Planning -** Confidential tax documents sent via email are permanently accessible to anyone who gains access to that account, even years later. Secure portals should be used for all tax-related document exchange.
- **Impact on Estate Planning -** Estate-related documents and communications shared via email are vulnerable to long-term exposure. Secure transmission methods protect the integrity of estate planning information.

Credit Freezes & Identity Monitoring
Page explained that individuals should assume some of their personal information is already publicly available, given the volume and frequency of data breaches. A complete personal profile — including Social Security number and tax records — can be purchased on the dark web for as little as approximately $125. Credit freezes (also referred to as credit locks) at all three major credit bureaus were described as a highly effective and low-cost protective measure. When a freeze is in place, no credit agency can pull a credit report, effectively blocking unauthorized credit extensions. Attendees were encouraged to freeze credit for family members — including children and grandchildren — who do not yet need access to credit. Paige noted she froze her son's credit within three months of his birth. Services such as LifeLock were discussed as a bundled option that can manage credit freezes, credit monitoring, VPN services, and password management across a household. One paid service was noted as sufficient; enrolling in multiple free monitoring services offered after breaches does not provide meaningfully better protection and introduces additional data-sharing exposure.

Dalal encouraged clients to take advantage of credit monitoring and freeze services proactively, rather than reactively. Extending these protections to family members — particularly minors — was highlighted as a straightforward and meaningful step.

- **Impact on Lifetime Portfolio Value -** Unauthorized credit activity or identity theft can result in financial losses and legal costs that affect long-term wealth. Credit freezes are a low-friction way to reduce this risk.
- **Impact on Projected Cash Flow -** Fraudulent credit accounts opened in a client's name can create unexpected debt obligations and cash flow disruptions.

- **Impact on Income Tax Planning -** Identity theft can extend to tax fraud, including fraudulent tax filings. Protecting personal information reduces exposure to this risk.
- **Impact on Estate Planning -** Protecting the credit and identity of family members — including minors named in estate plans — is an important component of comprehensive estate planning.

Password Management & Account Security
The session covered best practices for password management in detail. Key points included: never reusing the same username and password across multiple accounts; using a paid password manager (free versions were discouraged, as they are often used for security testing and may offer less protection); and understanding that paid password managers use multiple layers of encryption so that even in the event of a breach, actual credentials are not exposed. The Apple Keychain (iPhone) and Google Keychain were noted as safe options for users who access accounts exclusively from those devices, as they are effectively built-in password managers protected by biometric authentication. However, these do not extend protection to other devices (e.g., a home computer or a hotel computer). Attendees were advised never to log into accounts from shared or public computers. Password managers can also be configured to designate a trusted contact or inheritance access, allowing a family member to access accounts if needed — a feature Page noted she uses for her parents. Paid AI tools (e.g., ChatGPT, Gemini) were also mentioned: paying for the service (approximately $120/year) provides better default security than using the free version.

Clients were encouraged to use strong, unique passwords and a paid password manager are foundational elements of a personal cybersecurity program. Clients who find password managers difficult to manage should at minimum ensure they are not reusing passwords across accounts.

- **Impact on Lifetime Portfolio Value -** Weak or reused passwords are a primary entry point for account takeover, which can result in unauthorized access to financial accounts and direct asset loss.
- **Impact on Projected Cash Flow -** Unauthorized account access can lead to fraudulent transactions that disrupt cash flow and require time-consuming remediation.
- **Impact on Income Tax Planning -** Access to financial accounts through compromised passwords can expose tax-sensitive information and enable fraudulent tax activity.

- **Impact on Estate Planning -** Password manager inheritance features allow designated family members to access accounts in the event of incapacity or death, supporting continuity in estate administration.

Multi-Factor Authentication
Multi-factor authentication (MFA) was discussed as an important additional layer of account security. When given a choice, attendees were advised to have authentication codes sent to their phone rather than their email, since email is the most commonly compromised channel. Authenticator apps and text-based codes were described as roughly equivalent in effectiveness, and both are preferable to email-based codes. Page noted that she uses a dedicated email address — separate from her general email — as her recovery and authentication email for important accounts, so that authentication codes are not routed to her primary, more widely used inbox. Passkeys were briefly discussed: when a website creates a passkey on a recognized device, it is effectively building multi-factor authentication into the login process. Attendees were also reminded that if MFA verification (e.g., CAPTCHA) becomes frustrating, they can typically choose an alternative authentication method rather than abandoning the process.

Clients were encouraged to use an MFA on all financial accounts — and directing codes to a phone rather than email — is one of the most accessible and effective steps clients can take to protect their accounts.

- **Impact on Lifetime Portfolio Value -** MFA adds a meaningful barrier against unauthorized access to investment and financial accounts, reducing the risk of asset loss.
- **Impact on Projected Cash Flow -** Preventing unauthorized account access through MFA reduces the risk of fraudulent transactions that could disrupt cash flow.
- **Impact on Income Tax Planning -** MFA on tax-related accounts and portals helps prevent unauthorized access to sensitive tax information.
- **Impact on Estate Planning -** Securing accounts with MFA protects estate assets from unauthorized access, particularly important for accounts that are part of an estate plan.

Wire Transfer & Real Estate Transaction Fraud
A real-world fraud case involving a $4 million home purchase was discussed in detail. In that case, a fraudster had compromised the email of someone in the transaction chain (potentially the buyer, CPA, attorney, or title company) and monitored the transaction

over several months. When it came time to wire funds, the fraudster substituted a fraudulent account number while keeping the title company's name unchanged, and the client was pressured not to allow the advisor to call the title company to verify. The funds were wired to a fraudulent account and quickly divided across multiple accounts to evade detection. Some funds were ultimately recovered due to the speed of the response. ***The key takeaway:*** always call the title company or closing attorney directly — at a known, legitimate phone number — to verbally verify the account number before any wire transfer is initiated. Dan noted that his practice is to speak with both the closing attorney and the title company to validate all numbers verbally, which was affirmed as the most effective way to close the loop on this risk. Attendees were also reminded that Schwab will not act on emailed or texted wire instructions alone; verbal verification is required and is a deliberate fraud-prevention measure.

For any large financial transaction — particularly real estate purchases — clients should treat every wire instruction as potentially compromised until verbally verified with the receiving party at a confirmed legitimate number. The firm will always support clients in taking the time needed to verify before moving funds.

- **Impact on Lifetime Portfolio Value -** Wire fraud on large transactions can result in immediate, significant, and potentially unrecoverable asset loss. Verbal verification is a critical safeguard.
- **Impact on Projected Cash Flow -** A fraudulent wire transfer of this magnitude can materially disrupt a client's financial plan and liquidity position.
- **Impact on Income Tax Planning -** Fraudulent transactions may create complex tax situations, including questions around deductibility of losses, that require careful planning.
- **Impact on Estate Planning -** Large real estate transactions are often significant components of an estate plan; protecting the integrity of these transactions is essential to preserving intended estate outcomes.

Resources

If you suspect you are a victim of fraud, please immediately contact:

Charles Schwab: 888-3-SCHWAB
Salomon & Ludwin: 804-592-4999

Disclosures: Please remember that past performance may not be indicative of future results. Different types of investments involve varying degrees of risk, and there can be no assurance that the future performance of any specific investment, investment strategy, or product (including the investments and/or investment strategies recommended or undertaken by Salomon and Ludwin, LLC ["Salomon and Ludwin"]), or any non-investment related content, made reference to directly or indirectly in this blog will be profitable, equal any corresponding indicated historical performance level(s), be suitable for your portfolio or individual situation, or prove successful. Due to various factors, including changing market conditions and/or applicable laws, the content may no longer be reflective of current opinions or positions. Moreover, you should not assume that any discussion or information contained in this blog serves as the receipt of, or as a substitute for, personalized investment advice from Salomon and Ludwin. To the extent that a reader has any questions regarding the applicability of any specific issue discussed above to his/her individual situation, he/she is encouraged to consult with the professional advisor of his/her choosing. Salomon and Ludwin is neither a law firm nor a certified public accounting firm and no portion of the blog content should be construed as legal or accounting advice. A copy of the Salomon and Ludwin's current written disclosure Brochure discussing our advisory services and fees is available for review upon request or at www.salomonludwin.com. **Please Note**: Salomon and Ludwin does not make any representations or warranties as to the accuracy, timeliness, suitability, completeness, or relevance of any information prepared by any unaffiliated third party, whether linked to Salomon and Ludwin's web site or blog or incorporated herein, and takes no responsibility for any such content. All such information is provided solely for convenience purposes only and all users thereof should be guided accordingly. **Please Remember:** If you are a Salomon and Ludwin client, please contact Salomon and Ludwin, in writing, if there are any changes in your personal/financial situation or investment objectives for the purpose of reviewing/evaluating/revising our previous recommendations and/or services, or if you would like to impose, add, or to modify any reasonable restrictions to our investment advisory services. Unless, and until, you notify us, in writing, to the contrary, we shall continue to provide services as we do currently. **Please Also Remember** to advise us if you have not been receiving account statements (at least quarterly) from the account custodian.