



CYBER SECURITY MEMO

One of the responsibilities of SIRVA's cybersecurity team is to identify and combat the constant barrage of new cybersecurity threats. As part of SIRVA's continuing efforts to maintain security and keep our customers informed of important developments in the area of cybersecurity, we want to ensure that you are aware of and understand steps that you can take to mitigate risk.

Scams have occurred through which criminals have attempted to falsify banking instructions used in online transactions. Perpetrators may infiltrate an email account or even the computer of one of the parties to the transaction. Once infiltrated, the perpetrator then creates an email account that mimics the account of the real sender. The perpetrator then sends fake emails that have fraudulent wire or ACH banking instructions. This can result in significant financial loss. In some circumstances, the perpetrator intercepts and deletes emails between the actual parties involved in the transaction. Although cyber threats may emerge at any time or in any location, this type of hacking is currently emerging as a particular problem among real estate transactions in North America.

To minimize the risk associated with internet-based financial transactions, SIRVA has instituted new internal procedures to directly combat the efforts of hackers to falsify banking instructions.

In addition, we have listed some steps below that you can take to protect yourself from this type of theft. These steps are not applicable to all situations, but have proven effective in minimizing the risk of cyber theft. Above all, the key is to remain vigilant when conducting financial transactions and related activities and to immediately report any suspicious activity.

- Maintain updated cybersecurity subscriptions or software (commonly called, "antivirus software") for your computer that includes protection against email hacking. Most major email providers such as Yahoo, MSN, Google, and AOL have strong cybersecurity for email activity within the domain servers themselves. However, this protection does not filter down to your desktop computer, laptop, or other portable computers. You should not rely solely on your email provider's cybersecurity protection. Purchase a cybersecurity protection software or subscription that provides you with constant updates to address all the new threats that are out there.
- Often, company email systems maintain state-of-the-art cybersecurity protection software. Talk to your company about those protections and consider using a company-protected computer and your company email account for all matters involving your relocation activity.
- When working with Sirva or its suppliers, we expect our team members and suppliers to use their company email accounts. Please let us know if they are not doing so.
- Try to limit your internet activity to known sites that represent that they have cybersecurity features. Do not visit sites that are questionable, have lots of pop-up ads, or direct you to other websites.

- When sending or receiving financial information, verbally confirm that information that has been transmitted with a known source at the sender/receiver. If you do not know the sender or receiver of the email or have not had previous contact with them, then contact a known source (your relocation counselor or your broker) to confirm the contact name and number.
- Anytime you send funds, make sure the recipient is aware that the funds are coming and that they are on the lookout for the funds. Confirm that all funds that are sent via a one-time wire or ACH as soon as the funds are sent.
- When sending funds electronically (as opposed to sending a bank check) to cover a significant financial transaction, consider wiring the funds as opposed to an ACH. The wire will have a cost, but has additional security features including matching the account name to the number.
- Look closely look at the address of all emails you receive (including putting your cursor over the address) to help ensure that they are legitimate and not from a fraudulent account. (For example, if the email is supposed to come from “agent@broker.com,” look carefully to make sure the email does not read “agent@broker.co” or some other variation.) While not fail-proof, it is yet another step that you can take to help prevent fraud.
- Verbally follow up all email communication (or other secure transmission) that contains any financial information or instructions and confirm the accuracy or receipt of such information.
- It is unlikely that you will ever be asked to change banking directions. If you receive instructions to change banking information or provide new information, contact a known source to question and confirm any such change.
- Immediately report all suspicious activity to your bank, the local authorities, Sirva, and any other involved party as soon as you can. The sooner fraud is identified, the better the chance to stop it.

There are many benefits to the electronic transfer of funds via a wire or ACH transaction. However, these types of transactions are prone to cybersecurity scams. To avoid being scammed, it is critical that you use secure means to deliver and receive banking instructions and personal information, and follow secure verification procedures.

PLEASE BE AWARE THAT NEITHER SIRVA NOR YOUR BANK SHOULD PROVIDE YOU WITH WIRE INSTRUCTIONS. ONLY THE FUNDS RECIPIENT SHOULD PROVIDE YOU WITH WIRE INSTRUCTIONS. SIRVA WILL ONLY ACCEPT BANKING INSTRUCTIONS FROM YOU VIA OUR SECURE INFORMATION PORTAL. IF YOU ARE UNABLE TO PROVIDE THE INFORMATION VIA OUR SECURE INFORMATION PORTAL, CONTACT YOUR SIRVA CONSULTANT VIA TELEPHONE TO DISCUSS THE BEST WAY TO PROVIDE THE INFORMATION. WHENEVER INFORMATION OR MONEY IS SENT OR RECEIVED OUTSIDE OF OUR SECURE INFORMATION PORTAL (EITHER WITH SIRVA OR ANOTHER PARTY), IMMEDIATELY CONTACT THE OTHER PARTY TO VERBALLY CONFIRM THE ACCURACY OF INFORMATION AND BANK ACCOUNT INSTRUCTIONS WITH A PREVIOUSLY-KNOWN SOURCE AT THE SENDER/RECEIVER, AND TO ALSO VERIFY THE

AMOUNT OF FUNDS SENT OR RECEIVED BY THE COUNTERPARTY TO THE TRANSACTION. DO NOT SEND FUNDS UNTIL YOU HAVE VERBALLY CONFIRMED WITH A PREVIOUSLY-KNOWN SOURCE THAT THE INSTRUCTIONS HAVE BEEN PROPERLY TRANSMITTED.

Sirva is committed to delivering the best possible relocation experience through our mobility expertise, personalized support, and tools and resources to mitigate challenges every step of the way. Please contact your SIRVA representative should you have any questions about this communication.

John Kirk
Chief Information & Technology Officer
Sirva Worldwide, Inc.