UNITED BANK

FRAUD VICTIM GUIDE

If you are a victim of a scam, identity theft or other fraud schemes, the following steps are recommended in accordance with the Federal Trade Commission guidelines (Depending on the type of fraud, some of these steps may not be applicable.)

If you paid a scammer because of a scam (i.e. cash withdrawal, check, ACH, Wire)

1. Please contact your bank immediately to report the fraud and provide details on the transaction and scam.
2. File a complaint with the FBI's Internet Crime Complaint Center (IC3).
   Visit **www.ic3.gov** and file the FBI's Internet Crime Complaint.
   If funds were sent, provide information about the transaction and the scam itself. It's a good idea to add all transaction details and any additional information pertaining to the scam. Once you have filed the complaint, please be sure to print a copy for your records and for additional law enforcement reporting, if applicable.
3. File a police report with local authorities.
4. Save the incident number or police report number. Notify them that you completed an IC3 complaint.
   Exchange contact information with local authorities for future communication.

If funds were sent via Wire Transfer or ACH Payment due to an 'email compromise' or 'account takeover'

1. Please contact your local FBI and Secret Service Field offices.
   For FBI field office visit: **https://www.fbi.gov/contact-us/field-offices**
   For Secret Service field office visit: **https://www.secretservice.gov/contact/field-offices**
2. File a police report with local authorities.
3. Save the incident number or police report number. Exchange contact information with local authorities for future communication.
4. Engage IT experts, your system administrator or your internet provider to "Stop the Spread."
   Account takeover scams involve fraudsters gaining access to your computer or device, email system or server. These scams sometimes involve malware and fraudsters may corrupt your files.

Additional steps for Business Customers: Educate your employees

1. Implement cybersecurity awareness training programs.
2. Employ internal procedures to validate all payment requests or beneficiary account changes received through email and fax.
3. Verify all ACH and Wire requests by contacting the beneficiary directly with a previously established phone number, or in person, to confirm the request.
4. Do not rely on an email communication to send a payment.

Additional Guidance Provided by the Federal Trade Commission

Did you pay with a gift card?	Contact the company that issued the gift card. Tell them it was used in a scam and ask them to refund your money. Keep the gift card itself, and the gift card receipt.
Did you send a wire transfer through a company like Western Union or MoneyGram?	Contact the wire transfer company. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back. • MoneyGram 1.800.926.9400 • Western Union 1.800.448.1492 • Ria (non-Walmart transfers) 1.877.443.1399 • Ria (Walmart transfers) 1.855.355.2144
Did you send money through a money transfer app like *Zelle®*, PayPal, or Venmo?	Report the fraudulent transaction to the company behind the money transfer app and ask them to reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or card issuer bank. File a dispute/claim and ask to reverse the charge.
Did you pay with cryptocurrency?	Cryptocurrency payments typically are not reversible. Once you pay with cryptocurrency, you can only get your money back if the person you paid sends it back. Contact the company you used to send the money. Tell them it was a fraudulent transaction. Ask them to reverse the transaction.
Did you send cash?	If you send cash by U.S. mail, contact the U.S. Postal Inspection Service at 877.876.2455 and ask them to intercept the package. To learn more about this process, visit **https://www.usps.com/manage/package-intercept.htm.** If you used another delivery service, contact them as soon as possible.

If You Gave a Scammer Your Personal Information

Did you give a scammer your Social Security number?	Go to **IdentityTheft.gov** to see what steps to take, including how to monitor your credit.
Did you give a scammer your username and password?	Create a new, strong password. If you use the same password anywhere else, change it there, too.

If a Scammer Has Access to Your Computer or Phone

Does a scammer have remote access to your computer?	Update your computer's security software, run a scan and delete anything it identifies as a problem. Then take additional steps to protect your personal information.
Did a scammer take control of your cell phone number and account?	Contact your service provider to take back control of your phone number. Once you do, change your account password. Also check your credit card, bank and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution. Then go to **IdentityTheft.gov** to see what steps you should take.

Helpful Resources

National Crime Prevention Council
NCPC provides many brochures and valuable information to fight against financial crime such as Identity Theft, Protecting Private Information, Online Transactions and Seniors Against Crime.

United Bank is committed to helping prevent fraud and assisting you during a hard time if you are victim of a financial crime. If your account at United Bank is targeted by a fraud, please visit any of our branch offices or contact Customer Care.
800.327.9862 | **CustomerService@BankWithUnited.com**