



# Fraud Monitoring for ATM and Check Cards

## Frequently Asked Questions and Answers

---

**Q. Is this service 24 hours, or only in a certain window?**

**A.** In other areas of business, we have calls only going out during certain hours so cardholders aren't being called after normal waking hours. Emails will be sent 24 hours. Text will be sent from 7:00 a.m. to 10:00 p.m. in the cardholder's time zone. Calls will be sent from 8:00 a.m. to 9:00 p.m. in the cardholder's time zone. Texts and voice calls pending from the night before will be triggered the following morning at the applicable time noted above. Agents are available 24/7.

**Q. How can I stop text messages if I don't want to receive them any longer?**

**A.** All you need to do is respond back to the SMS text alert with the word STOP. U.S. consumers who have service through AT&T, Verizon, Sprint, and T-Mobile will not be charged message or data rates to receive our fraud alerts. We absorb that cost for you!

**Q. Will the product work for customers residing in Canada?**

**A.** For Canadian consumers, both text and email alerts are available.

**Q. Can the alerts be sent to customers travelling internationally?**

**A.** We are unable to send text or phone calls internationally, but please make sure your email address is current as we can always email you 24 hours a day 7 days a week.

**Q. How do customers enroll?**

**A.** We have already included you in these enhanced services as part of our fraud protection services.

**Q. What triggers these alerts?**

**A.** Transactions that we have identified as potential fraud trigger the alerts.

**Q. If I receive an alert, does that automatically block my account from further purchases?**

**A.** The majority of suspected fraud accounts will be blocked, just as they are today. However, some lower risk items may not be declined.

**Q. If I respond back that the transaction(s) are valid, will you automatically unblock my account?**

**A.** Yes, though please keep in mind that it could take 5 – 10 minutes for a block to be removed in some situations.

**Q. If a transaction is declined due to suspected fraud, but I validate that I did make the purchase, can I try to complete the purchase again?**

**A.** Once the alert is validated in our fraud system, you can attempt the transaction again, usually within 5 – 10 minutes of the initial call/text/email.

**Q. What if my "yes" or "no" text response has a typo?**

**A.** The system will accept many common typo variations of the "yes" or "no" text message response. If the system cannot understand what was typed, it will generate a message to call a representative for help.

**Q. Is there a difference for consumers and businesses cardholders?**

**A.** No.

**Q. Can I establish preferences through my mobile app?**

**A.** Alerts are not configured through a mobile app, but rather through our fraud systems. The standard order of engagement is: (1) Text (2) Voice Call (3) Email



Alerts generated overnight result in an email only until calling and texting hours are available. Text will be sent from 7:00 a.m. to 10:00 p.m. in the cardholder's time zone. Calls will be sent from 8:00 a.m. to 9:00 p.m. in the cardholder's time zone.

**Q. How do incoming and outgoing voice calls work?**

**A.** Actions are triggered by today's existing fraud alerts through the Falcon system. If a mobile phone is on record, a text alert will be triggered first. All numbers on record that are identified as a mobile phone will be utilized. We have technology that allows it to determine if a phone number is a mobile or land line. If we do not receive a response to the text(s) within 30 minutes, the system sends an automated voice call asking you to confirm if authorizations are valid or unrecognized. If you select "Not Recognized," the call is transferred to an agent to confirm the fraudulent transaction(s). If there is no response within 5 minutes to the voice call, an email is sent requesting that you confirm the transactions are valid.

**IMPORTANT: United Bank will never ask for your account number, PIN number, card number or full Social Security number. If you get asked for this information, please do not provide it, hang up the call and contact us immediately at 800.327.9862.**

---

**SMS Text Example**

SMS Alert

FreeMsg: United Bank Fraud Dept 800.xxx.xxxx: Suspicious txn on acct 1111: \$201.99 WALMART. If authorized reply YES, otherwise reply NO. To Opt Out reply STOP.

If they reply YES the case will be closed as not fraud and they will receive the following response:

SMS Response to "YES"

FreeMsg: United Bank Fraud Dept: Thank you for confirming this activity. Your account is safe for continued use. To Opt Out reply STOP.

SMS Response to "NO"

FreeMsg: United Bank Fraud Dept: Thank you. We will call you or you can call us anytime at 800.xxx.xxxx. To Opt Out reply STOP.

If they reply NO the Automated Call System will generate an outbound call to the cardholder during available calling hours. The cardholder will be asked to identify security and the call will then be transferred to a Fraud Alert Specialist. The cardholder will also receive the following response:

SMS Response to "HELP"

FreeMsg: United Bank Fraud Dept: received your msg. It is important we talk to you. Please call 800.xxx.xxxx ASAP. To Opt Out reply STOP.

---

**Email Sample**

From: [FraudServiceCenter@UnitedBank.com](mailto:FraudServiceCenter@UnitedBank.com)

Subject: URGENT: Your Card Has Been Suspended Due to Recent Account Activity

Your Card Ending in xxxx

Dear (Cardholder Name):

As part of our commitment to protecting the security of your account, we continuously monitor for possible fraudulent activity. We need to verify that you, or someone authorized to use your account, attempted the following transaction(s) on your account ending in xxxx:



Merchant	Amount	Date	Time	Location
TRIGGER	\$440.01	04/01/2016	08:01 AM	MILWAUKEE, WI
WALMART	\$504.95	04/01/2016	10:02 AM	MILWAUKEE, WI
WALMART	\$104.95	04/01/2016	09:31 AM	MILWAUKEE, WI

If the dollar amount is not identical to what is shown on a transaction receipt, this may be due to a preauthorization which has not yet posted to your account.

The merchant location for internet transactions may be different than you expect as they are often cleared through a centralized billing location.

If you have already spoken with us about these transactions, then no further action is required.

Please click on one of the two statements below that best represents the transactions above:

[All Transaction\(s\) Authorized](#)

[One or More Transaction\(s\) NOT Authorized](#)

**NOTE:**

Your satisfaction is very important to us and we appreciate your prompt attention to this matter. If you have any questions about the content of this email, please don't hesitate to contact us at 800.xxx.xxxx from the U.S. and Canada. If you prefer, use the phone number on the back of your card. Internationally, you can reach us collect at 727.xxx.xxxx and we will accept the international collect call charges. For your convenience, we are available to take your call 24 hours a day, 7 days a week.

Thank you for being a valued customer.

Sincerely,  
United Bank Fraud Service Center

Please do not respond to this email, this mailbox is not monitored. It is only used for sending Fraud Alert Email notifications.

If they click the link "All Transaction(s) Authorized" then we will close the case as not fraud, remove any temporary block and they will be provided with the following message:

Dear (Cardholder Name):

Thank you for confirming this activity; your United Bank card is available for use. We appreciate your business and immediate attention to this matter.

Thank you for being a valued customer.

Sincerely,  
United Bank Fraud Service Center

If they choose the link "One or More Transaction(s) NOT Authorized" the Automated Call System will generate a call to their phone numbers on file (time-zone permitting) and then transfer them to a Fraud Alert Specialist after verifying security. Additionally, they will be provided the following message:

Dear (Cardholder Name):

Thank you for confirming this activity as not authorized by you or someone authorized to use your account. We will contact you shortly or you may call the following number: 800.xxx.xxxx. We are available 24 hours a day, 7 days a week.

Sincerely,  
United Bank Fraud Service Center