Regions Identity Theft Kit

How to protect yourself from identity theft, and what to do if you suspect you may be a victim.

REGIONS

Index

At Regions, we take customer security seriously.

We value the relationships we have built with you and your family and hope that you never become the victim of identity theft. But, because identity theft is such a fast-growing crime, we want you to be aware of the basic precautions you can take to protect yourself. We have created the Regions Identity Theft Kit to help you understand the crime and minimize the risk. Included are safety measures and tips on safeguarding your personal information, performing online financial transactions, browsing the Web securely, and protecting your identity online.

In addition to providing you with information on how to protect your identity, we have also included an important contact list and information on what to do if you suspect that you have been a victim of identity theft. An Identity Theft Action Register also has been provided to help document the steps you may have to take.

For more information about fraud and identity theft, as well as ways to protect yourself against them, please visit the Privacy & Security section at www.regions.com

What Is Identity Theft?

Identity theft occurs when a criminal takes your personal information — such as your name, address and Social Security Number — and uses it to establish or attempt to establish accounts or perform other transactions in your name (checking, savings, credit cards, loans, tax refunds, purchase of goods and services, etc.). Thieves can steal the information necessary to commit identity theft in a number of ways:

- From discarded bills or statements
- From a lost wallet
- From stolen mail
- By obtaining a copy of your credit report
- From fraudulent Internet, telephone or text messaging scams
- From information you might disclose on the Internet

How Identity Theft Works

Identity Theft can occur by using many different types of techniques. Some of the techniques are listed below:

Phishing

'Phishing" is a form of Internet piracy. It's pronounced "fishing," and that's exactly what these thieves are doing: "fishing" for your personal financial information. What they want are account numbers, passwords, Social Security Numbers, and other confidential information that they can use to loot your checking account or run up bills on your credit cards.

In a typical case, you'll receive an email that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the email may appear to come from a government agency, including one of the federal financial institution regulatory agencies. The email will probably warn you of a serious problem that requires your immediate attention.

It may use phrases such as "Immediate attention required," or "Please contact us immediately about your account." The email will then encourage you to click on a button to go to the institution's Website or reply to the email. In a phishing scam, you could be redirected to a phony Website that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual Website. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information.

In these cases, you may be asked to update your account information or to provide information for verification purposes: your Social Security Number, your account number, your password, your personal identification number (PIN), or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name, your date or place of birth, or answers to security questions.

If you provide the requested information, you may find yourself the victim of identity theft. Remember, REGIONS WILL NEVER ASK FOR THIS INFORMATION VIA EMAIL.

Please forward any suspicious emails to phishing@regions.com. We also recommend that you do not run any executable (e.g., .exe file) or .zip files received from an email unless it is from a known trusted source.

Vishing and Smishing

Variations of phishing scams include "vishing" and "smishing". In a vishing scheme, you would receive an email, supposedly from a reputable source, with an urgent request for you to call a phone number. You would then be asked to provide sensitive information either by voice or by entering digits. Smishing attacks employ text messages to your mobile device — again, apparently from a legitimate source and of an urgent nature — asking you to click on a link in a message and then provide sensitive information.

Phony Identity Theft Protection or Credit Repair Scam

Credit repair scams offer to erase negative information from your credit file so you can qualify for a credit card, auto loan, home mortgage, or a job. The Federal Trade Commission has warned that some companies claim to be identity theft prevention services but are, in reality, scam artists trying to get your driver's license number, mother's maiden name, Social Security Number and credit card and bank account numbers. The FTC has advised consumers not to give out any personal information over the phone or online unless you are familiar with the business that is asking for it. If you are unsure about a firm, check it out with the Better Business Bureau before divulging the information they are asking for.

The scam artists who promote these services can't actually do anything to help repair your credit. Be aware that they may recommend that you lie on a loan or credit application, misrepresent your Social Security Number, or get an Employer Identification Number from the Internal Revenue Service under false pretenses, all of which violate federal law.

"Your Account Needs to be Updated" Scam

These scams usually show up in your email inbox with a message from the "System Administrator" telling you to perform some urgent maintenance on your account or to verify your account information and Social Security Number. If this type of email contains a link, do not click on it.

Special Visa®/MasterCard® Scam

This scam involves a phone call from a Visa or MasterCard "employee" trying to confirm unusual spending activity. They will then ask for the three-digit "Security Code" on the back of your credit card. You should not give the code on the back of your credit card to anyone unless you have initiated the call and it is to a reputable merchant. If you are unsure, hang up and call the fraud number on the back of your card.

"Free Credit Report" Scam

Almost all of the "free credit report" emails you receive are scams. Either the person is trying to find out your Social Security Number or will be billing you for a service later on. Do your homework and check out the company via the Better Business Bureau and Federal Trade Commission.

If you provide the requested information, you may find yourself the victim of identity theft. Remember, REGIONS WILL NEVER ASK FOR THIS INFORMATION VIA EMAIL.

Dumpster Diving

Believe it or not, there are criminals who go through the trash of businesses or residences hoping to find confidential information about consumers. They may also visit dumpsters in hopes of finding records, mail, or other papers that have been thrown away. Shred any documents containing sensitive information.

Stealing from Mailboxes

Criminals will steal mail from mailboxes, both items placed there as outgoing mail by a resident or delivered by the postal carrier. The identity thief is looking for credit card bills, bank statements, credit card offers, and other mail that may contain personal identifying information.

What You Can Do To Protect Your Identity

There are steps you can take to protect yourself and your identity. Below are some basic reminders, including how to protect yourself online:

- **Bank and Credit Statements**

  Review your bank and credit statements promptly and report any discrepancies or suspicious transactions immediately. Also, report any discrepancies you notice while performing other routine transactions (i.e., ATM transactions, online sessions, etc.). Report lost or stolen checks, credit cards, and ATM/check cards as soon as you discover they are missing.

- **Monitor Your Credit Report**

  Monitor your credit report annually for inquiries and accounts that you are unfamiliar with. You are entitled to receive one free credit file disclosure every 12 months from each of the nationwide consumer credit reporting companies — Equifax, Experian and TransUnion. This free credit file can be requested through annualcreditreport.com or by calling 877-322-8228.

  You have the option of ordering all three at the same time (which allows for comparison of data maintained by the three companies) or ordering one from each of the three companies at periodic intervals (which may alert you to any changes in your credit report).

- **Use Precautions With Your Mail**

  Make a habit of placing outgoing mail containing payments or sensitive information in a collection box or at your local post office. If you are going to be out of town or unable to pick up your incoming mail, ask a friend to retrieve your mail or request your Post Office to hold it for you. To make sure your statement is secure, consider moving from paper to an electronic format. You can enroll in Regions Online Banking with online statements at www.regions.com.

- **Use Precautions With Your Trash**

  Consider investing in a shredder. Don't make the mistake of carelessly tossing out credit card statements with courtesy checks enclosed, credit card offers, mail, or any other paperwork that may contain personal information. Shred these items or tear them up finely so that a "dumpster diver" won't be able to glean any facts from your trash.

- **Know Your Caller**

  Remember that identity thieves are skilled criminals who may use many different ruses to obtain information over the phone. They may pose as someone from your bank, credit union, utility company, or other company that you are known to frequent. Unless you have initiated the call, don't give out any personal information over the phone to someone unknown to you.

- **Safeguard Your Personal Information**

  Your Social Security Number (SSN), credit card numbers, and other sensitive information are key pieces of information sought by identity thieves. Use good judgment in where and how you carry this information with you. For example, you generally don't need to carry your Social Security Card with you, and you may only need to carry one credit card rather than multiple cards. Consider storing unneeded information in a secure location in your home or safe deposit box rather than in your purse or wallet.

- **Online IDs and Passwords**

  Never provide your online passwords over the phone or in response to an unsolicited Internet or email request. Regions will never ask you to verify your account information via email, nor will we ask for your online password via phone. Online IDs and passwords are highly confidential and should never be given to anyone. Make sure that you choose ones that will be easy for you to remember but very difficult for someone else to guess, and never write your password down on a piece of paper. Don't use the last four digits of your Social Security Number or any other personal information as your online ID or password. Change your password every month or two. If someone has learned your password, change it immediately.

- **Online Banking Security Questions**

  If you use Regions Online Banking, do not give anyone the answers to your security questions. These questions are designed to protect your accounts from unauthorized access. One of these questions may be asked if our system detects an attempted login that falls outside of your usual pattern.

- **Divulging Personal Information on the Web**

  As you surf the Web and find sites that you enjoy, you may be asked to fill out forms and give personal information. Make sure you are aware of the company's privacy policy. If you do not "opt-out," they may sell or share your information with other parties.

Remember, Regions will not contact you by phone or by email to ask for or to verify your Online Banking Customer Number, PIN or any other sensitive information. If you contact the bank, however, we will ask for information that will allow us to verify your identity so we can ensure your privacy.

- Monitor Your "Cookies"

  "Cookies" are small files that Websites place on the hard drive of your PC to access the next time you visit their site. For sites that you visit frequently, cookies keep track of what you've done there before and to make your browsing preferences more automated.

  Monitor all your cookie transactions by setting the security preferences on your browser to prompt you before accepting any cookies.

- Shopping Online

  Know the merchant. Purchase from only those companies that you feel comfortable with or those that take extra steps to communicate their honest intentions to you through transparent policies and seals from consumer organizations. The Federal Trade Commission maintains a Website, consumer.gov, which includes buyer's guides, tips, and links to helpful resources.

  Use a credit card. It's a good practice to pay with credit cards, because under federal law (and your credit card agreement) your liability for an unauthorized charge is limited to $50. When using a credit card online, do not give your credit card number unless you are entering it into a Web page that will encrypt the number. You should see "https" in the Web address, and the padlock symbol should also appear on your screen.

- Banking Online

  Bank Web sites are usually divided into two sections: the public Website that anyone can access and the secure Website that requires some combination of identification and passwords and can only be accessed by customers of the bank. As mentioned in the section on Browsers, if you are viewing or sending private information, look for secure or encrypted connections signaled by the "https" in the address bar of the browser or a closed padlock icon. Also, make sure that you don't pass any personal information through a bank's Website except through a secure connection. If you do, you run the risk that someone else may intercept that information.

Before moving on to the next Website, be sure to end your online banking session by logging out. If you don't log out, your online banking session will continue until it automatically times out, which could take several minutes. In most cases, if you move on to another Website without logging out, your banking information can still be accessed simply by clicking the Back button on the browser if you leave your computer unattended.

- **Paying Bills Online**

  You should pay your bills only through a secure online connection. As long as you protect the identity of your online banking ID and passwords, online bill payment is designed to be secure.

- **Browse the Internet Securely**

  Browsers are simply computer programs that your computer uses to communicate with Web servers and display Web pages. Information that you access on Websites travels between your computer and a Web server through a series of computers and it's not known to you which computers are going to handle your information. Therefore, several protection mechanisms have been created to ensure the secure transmission of your sensitive data. Encryption is one way of safeguarding your information when transmitted over the Internet. Encryption is the process of transforming data into a form unreadable to anyone except those who possess the decryption key.

  — **How does encryption work?**

  Before information leaves your computer, it's coded using a special "key" that makes the information unreadable. While this scrambled information travels over the Internet, it is extremely difficult and impractical to decipher. Once it reaches its final destination, it's decoded using another special "key" and turned back into a form that can be used.

  — **How do I stay updated on browser security?**

  Be sure you are running the most updated, secure browser available to take advantage of the latest anti-malware to protect you from viruses, worms, and spyware delivered over the Web. There are two types of secure browsers available to you at present: 40-bit encryption and 128-bit encryption. Regions requires 128-bit encryption, which is the strongest form of encryption. Many security experts recommend keeping your Internet browser updated with the latest version available.

- More Browser Safety Tips
  - Never open more than one browser or visit another, non-secured Website while engaging in a secure online transaction.
  - Always close and restart your browser before and after using a secure session.
  - Turn off your "scripting behaviors" in your browser. Some Websites will not open with the scripts disabled and you may have trouble with your Web mail service. If so, you will need to set up URLs to get these working again. Again, reference your computer manual for directions or contact your help line to walk you through this process.
  - Set up software and hardware firewalls. Software firewall programs can be purchased relatively inexpensively.
  - Disconnect from the Internet when you are not actively using it. Leaving your Internet connection open is like leaving your front door wide open all day and all night. If you leave your Internet open, anything can come in, anytime! Again, make it a habit to close your session.
  - If you are browsing a Regions Website and get a warning about an invalid security certificate, this should be a red flag and could indicate a malware infection on your computer. Please contact Online Banking Customer Service immediately at 1-800-472-2265.
- Control Spyware

  Spyware is a hidden program that is installed on a computer without the consent of the owner to secretly gather personal data. The information can then be used by advertisers or even hackers. Spyware can monitor keystrokes, passwords, credit card numbers, Websites visited, and more. Virtually anything on your computer is available to spyware unless you protect yourself.

  It is very common that spyware programs are poorly written and in many instances contain bugs that cause malfunctions of your computer such as unexpected crashes or a noticeable slowdown in performance. One way of protecting your computer is to uninstall software that you are no longer using. This is a good practice and will enable you to notice any new software that was loaded without your authorization.

Another means of being proactive is to always review the privacy policy of the company and the fine print of the license agreement before installing software. Spyware companies work hard to disguise their intentions and it is just as important to know how legitimate companies plan to use the information they collect.

Keep in mind that installing antivirus programs does not fully protect your computer from spyware. Utilizing specialized anti-spyware software is the best means of protection. Also, anti-malware software can help protect you from a variety of types of malicious code, typically including spyware and viruses.

What Regions Is Doing To Protect Your Identity

Regions follows strict information security procedures designed to protect the confidentiality of your information. We also use the latest technology to ensure the confidentiality of your banking data. Advances in security technology occur frequently, and Regions continually evaluates our security environment to ensure that it provides the highest level of privacy and safety for our customers. We put the highest priority on protecting the safety, soundness, and security of financial transactions and the systems that those transactions depend on.

General Account Security

- Regions monitors check, debit card, wire and ACH (electronic payment) activity to look for suspicious activity on your accounts.

Regions' Online Banking Security

- Regions' online products use the latest encryption technology to secure your data over the Internet. Encryption is the process of transforming data into a form unreadable to anyone except those who possess the decryption key.
- For your protection, Regions uses 128-bit encryption throughout our Regions Online Banking Website. If your browser doesn't support 128-bit encryption, you can download a new browser for free.
- Regions uses multifactor authentication to protect your accounts through Online Banking. If our system detects an attempted login that varies from your usual pattern, you will be prompted to answer one of your previously established security questions.

- Regions uses digital certificates to assure that when you access our secured Websites, you are actually communicating with Regions and not an imposter.
- If you receive an email asking you to log into Regions Online Banking and it does not link to our official Regions Online Banking site at regions.com, do not divulge any personal information in response to that email or in any Web page that email links to.
- Remember, our emails will always link to Regions Websites. When we link to Regions Online Banking from an email, the Address bar at the top of your browser will always look like this:

- Any email you receive from Regions containing a link will also include the last four digits of your account number to help you ensure its authenticity.
- Regions Online Banking is a secure site so there will always be a locked padlock displayed in the lower right hand corner of your browser. Please do not divulge any personal information to a Website that does not display this locked padlock:  . Make sure you check for the other hints listed here, as this padlock can be faked. If in doubt, go directly to regions.com from a separate browser session.
- Regions does not use emails or popup windows in Regions Online Banking to ask for information from you.
- When we link to applications from our emails, the information in the address bar at the top of the browser will always contain “regions.com.”
- Regions’ servers are physically secured and monitored 24 hours a day. They are also protected by Internet firewalls.
- A sign-on is required before access is allowed to your data. Your PIN (Personal Identification Number) is displayed as asterisks when you enter it.
- To prevent unauthorized access to your accounts when you step away from your computer, your Regions Online Banking session automatically signs off after 10 minutes. It is best to sign off and close your browser after completing your banking session.

Whom To Contact If You Are or May Be a Victim of ID Theft

If you begin to get suspicious bills or phone calls from creditors about unknown debts, you may have been the victim of identity theft.

After verifying that the suspicious credit has, in fact, been opened using your personal information, you will need to do the following tasks:

1. The first thing to do is call the local police and file a report. Make sure to get a copy of the police report. You may need this copy to validate claims.
2. Call all of your credit card companies and your financial institutions to explain the situation. Close compromised accounts and open new ones. Information for contacting Regions is on the next page.
3. Contact your local Department of Motor Vehicles. You may want to get a new driver's license. Also, you will want to verify that a duplicate license was not recently issued in your name to an imposter.
4. Contact the Social Security Department at 1-800-269-0271 if you suspect your number was used to obtain fraudulent accounts.
5. Place a fraud alert on your credit reports and review each report by contacting the three credit bureaus listed below:
   - Equifax: 1-800-525-6285
   - Experian: 1-888-EXPERIAN (397-3742)
   - TransUnion: 1-800-680-7289
6. Contact the U.S.Postal Inspectors Office or your local Post Office to report any crime involving stolen mail or use of the mail as part of a fraud scheme.
7. Contact your health insurer to notify them of the theft, and to get a replacement card. Imposters may use your insurance card to obtain benefits. Your own health may be at risk if the imposter's health information is added to a profile under your name if they receive treatment.

8. File a complaint with the Federal Trade Commission. To file a complaint or to learn more about the FTC's Identity Theft initiatives, visit consumer.gov/idtheft. If you don't have access to the Internet, you can call the FTC's Identity Theft Hotline (toll-free): 1-877-IDTHEFT (438-4338); TDD: 866-653-4261; or write:

   Identity Theft Clearinghouse
   Federal Trade Commission
   600 Pennsylvania Avenue, NW
   Washington, DC 20580

Use the **Regions Identity Theft Action Register** provided in this kit to document your process.

How You Should Handle Your Regions Accounts

You should first review all of your accounts for any suspicious activity or transactions either online at regions.com or by calling 1-800-REGIONS (734-4667). If you have determined that your Regions accounts have been compromised or you suspect that a Regions account exists that you did not open, please contact a Regions Banker at 1-888-987-6540.

If you determine that your Regions accounts have not been compromised we recommend that you:

- Place a security password on all accounts. Doing so will assist us in keeping your information secure. Each time you contact us by phone, we will request your security password.
- Review the address, phone number, and email address on your accounts to ensure that we have the most accurate information.
- Verify that you have, in your possession, all checks and cards issued on your accounts.

Information adapted from the federal bank, thrift, and credit union regulatory agencies.

Beginning on the following page please complete the Uniform Affidavit for Identity Theft and fax it to (205) 261-6631, email it to idtheft@regions.com, or mail it to:

Regions Corporate Security
P.O. Box 10105
Birmingham, AL 35202

If you have any questions, please call (205) 261-0140.

Uniform Affidavit for Identity Theft

Victim Information

1. My full legal name is

_____
(First) (Middle) (Last) (Jr., Sr., III)

2. (Complete if applicable.) When the events described in this affidavit took place, I was known as

_____
(First) (Middle) (Last) (Jr., Sr., III)

3. My date of birth is _____ 4. My Social Security number is _____
Month Day Year

5. My government-issued identification (passport, driver's license, state identification, matricula, visa or green card) information is

Check one ☐ Driver's License _____
☐ State Identification State Number Issue Date (month/date/year) Expiration Date (month/date/year)

Check one ☐ Passport ☐ Matricula ☐ Visa ☐ Green Card _____
Number Issue Date (month/date/year) Expiration Date (month/date/year)

6. My current street address is

_____
Number & Street Name Suffix (Apartment, Suite, etc.)

_____
City State Zip Code

7. I have lived at this address since _____
Month Year

8. (If different from above.) When the events described in this affidavit took place, my address was

_____
Number & Street Name Suffix (Apartment, Suite, etc.)

_____
City State Zip Code

9. I lived at the address in #8 from _____ until _____
Month Year Month Year

10. My daytime telephone number is _____ My evening telephone number is _____

My email address is _____

How the Fraud Occurred

Check all that apply for #11 – #13

11. ☐ Did Identity Theft occur with Regions Bank? ☐ Yes ☐ No
(if No list the Financial Institution where the fraud occurred _____)

12. ☐ I did not receive any benefit, money, goods, or services as a result of the events described in this report.

13. ☐ My identification documents (for example: credit cards, birth certificate, driver's license, Social Security card, etc.) are/were:

☐ still in my possession ☐ stolen on or about ☐ lost on or about _____
Month Day Year

(continued on next page)

Uniform Affidavit for Identity Theft

Check #14 or #15 as applicable

14. ☐ To the best of my knowledge and belief, the following person(s) used my information (for example: my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to conduct financial transactions, cash checks, make withdrawals or to obtain money, goods or services without my knowledge or authorization.

Name _____
(First) (Middle) (Last) (Jr., Sr., III)

Address _____
Number & Street Name Suffix (Apartment, Suite, etc.)

_____
City State Zip Code

Phone number(s) _____

Other information _____

_____

15. ☐ I do NOT know who used my information or identification documents to conduct financial transactions, cash checks, make withdrawals or to obtain money, goods or services without my knowledge or authorization as described in this report.

16. ☐ Additional comments (for example: description of the fraud, documents or information used, or how the identity thief gained access to your information).

_____

_____

_____

Victim's Law Enforcement Actions

17. Check one: I ☐ AM ☐ AM NOT willing to assist in the prosecution of person(s) who committed this fraud.

18. Check all that apply: I ☐ HAVE ☐ HAVE NOT reported the events described in this affidavit to the local police department.

The police ☐ DID ☐ DID NOT write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

_____
Police Department Report Number, if Any Report Date (month/date/year)

_____
Phone Number Email Address, if Any

Documentation Checklist

Please indicate the supporting documentation you are able to provide to verify your identity. Attach copies (NOT originals) to the affidavit before sending it to your financial institution.

19. ☐ A copy of a valid government-issued photo identification card (for example: your driver's license, state-issued ID card or your passport).

20. ☐ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example: a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

Signature

I certify that, to the best of my knowledge and belief, all of the information on and attached to this Affidavit is true, correct, and complete and made in good faith. I also understand that this Affidavit or the information it contains will be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. § 1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

Signature _____

Date _____

Regions Identity Theft Action Register

This simple form will aid you in tracking your progress as you work through the different processes. Make sure to be detailed and precise when listing the information and most importantly, always follow up. You must be as meticulous as the people who stole your information.

Police Contact

Police Department	Phone Number/ Address	Contact Date(s)	Contact Name	Notes

Financial Account Contacts

Bank/Credit Card/ Investment	Phone Number/ Address	Contact Date(s)	Contact Name	Notes
Regions Bank	1-800-REGIONS (734-4667)			

Motor Vehicle Department

Department	Phone Number/ Address	Contact Date(s)	Contact Name	Notes

Social Security Department

Department	Phone Number	Contact Date(s)	Contact Name	Notes
Social Security Department ID Theft Hotline	1-800-269-0271			

Credit Bureau Contacts

Bureau	Phone Number	Contact Date(s)	Contact Name	Notes
Equifax	1-800-525-6285			
Experian	1-888-EXPERIAN (397-3742)			
TransUnion	1-800-680-7289			

Federal Trade Commission

Department	Phone Number	Contact Date(s)	Contact Name	Notes
Federal Trade Commission	1-877-IDTHEFT (438-4338); TDD: 866-653-4261			

Health Insurer Contacts

Department	Phone Number	Contact Date(s)	Contact Name	Notes

United States Postal Inspector

Department	Phone Number	Contact Date(s)	Contact Name	Notes

It's time to expect more.

1-800-REGIONS | regions.com