GBA

GEORGIA BANKERS ASSOCIATION
the resource that empowers

Resource Sheet
Communications Guide

Joe Brannen I President and CEO I 404.420.2026 I jbrannen@gabankers.com
David Oliver I SVP-Communications and Marketing I 404.420.2036 I doliver@gabankers.com
Web site I www.gabankers.com

Updated July 8, 2016

Tips for Consumers to Protect Against Fraud

Any time there's a big data theft announced, bank customers are interested to know what they can do to protect their accounts and sensitive information. Banks use a variety of safeguards to protect your information and prevent fraud, such as special fraud detection software, sophisticated computer security systems, employee training and strict privacy policies. Here are some important tips for consumers who are worried their information may have been compromised:

How to Protect Your Identity and Accounts…

- Watch your account like a hawk. Monitor your account transactions online frequently. Set up electronic transaction notifications and balance alerts through your bank's online banking service to monitor activity. Check your statement every month.

- Notify your bank immediately if you notice a fraudulent transaction. You will be reimbursed for verified fraud if you report it promptly.

- Be alert for phishing scams trying to trick you out of giving up account numbers and other information. They often arrive as email, phone or text messages asking for your account number or other details. Banks and credit card companies already have that information and won't ask you for it in such unsolicited requests. Call your bank directly or navigate to their official website from a separate browser page if you're suspicious.

- Change your password regularly and avoid using a similar password for your bank accounts as you do for other websites or apps. Don't use common numbers such as birthdates, street addresses or other information that can be easily associated directly with you in your passwords. Don't keep a list of passwords, PINS or usernames in your wallet or in an unsecure computer file.

- Don't give your Social Security number or other personal credit information about yourself to anyone who contacts you.

- Order free copies of your credit report once a year to ensure accuracy.

- When using social networking sites, never include personal contact information including telephone numbers, Social Security number, birth date, email addresses, physical address, mother's maiden name or other information that could provide sensitive information to fraudsters or hints to passwords.

- Don't open email from unknown sources and use virus detection software. Banks won't send you an email asking you to click on a link and provide sensitive account information.

- Consider signing up for identity theft protection services. If your information is confirmed by a company to have been compromised, it will usually provide the service to you for free. Look for information directly from the company and read all communication carefully.

– more –

Consumer tips for fraud protection, continued

What to Do if You're a Victim of Fraud…

- Contact your bank immediately if you know or suspect your account has been compromised or you identity has been stolen. Use the tools it has to help you.

- File a police report and contact the three major credit reporting companies. The fraud unit numbers are:
  - TransUnion – 800.680.7289
  - Experian – 888.397.3742
  - Equifax – 800.525.6285

- Keep records of your communication with authorities, including names and contact numbers.

- For more advice, contact the FTC's ID Theft Consumer Response Center at 1-877-ID THEFT (1-877-438-4338) or http://www.ftc.gov/idtheft.

Background: Banks Act Swiftly to Protect Customers when Fraud is Detected or Suspected.

- Many banks have special fraud detection software that constantly monitors accounts to help flag ID theft.

- If a bank detects possible fraud or if it is contacted about potential fraud, it immediately takes action by closing accounts when appropriate and beginning an investigation. Depending on the data that is compromised, the bank may take a variety steps such as:

  - Enhanced account monitoring and customer notification
  - Blocking account access and re-issuing cards
  - Reimburse customers for confirmed fraudulent transactions.

- Due to the zero-liability fraud protection offered by most banks and credit card companies, most victims do not experience any out-of-pocket costs from fraudulent transactions.

- Banks bear the cost of account fraud, not consumers. Reimbursing customers and re-issuing cards can cost millions of dollars. For example, the Target data breach in late 2013 cost banks and credit unions $200 million just to re-issue cards, according to data collected by the Consumer Bankers Association and Credit Union National Association. The cost estimate does not include reimbursement for actual fraudulent charges.

- Beyond the monetary cost, banks bear significant reputational risk if their account protection efforts, customer service and communication efforts about fraud are not excellent. Banks have become proactive and effective at dealing with these issues.

- Most banks have special toll free numbers and websites devoted to helping victims of identity theft.

- Many banks offer special worksheets, phone numbers and standardized affidavits to send to other businesses that may need to be contacted. A special affidavit is available from the Federal Trade Commission at www.ftc.gov/idtheft.