What the Bank is Doing

Bank of Hawaii provides identity theft victims with responsive, caring service from beginning to end. When notified by a customer of a possible identity theft, Bank of Hawaii will ensure that accounts are closed and protected properly. Designated staff members will also follow up with customers and monitor accounts for any suspicious activity. Our goal is to ensure that customers experience complete resolution and consistent follow-through so their concerns and issues are handled in a timely and caring manner.

ONLINE SERVICES

At Bank of Hawaii, we constantly strive to make improvements to our systems and processes to ensure the quality, safety, and integrity of your online banking experience. To do so, we use the latest technology – including cryptographic techniques, firewalls, and trusted operating systems to ensure that your Internet transactions with Bank of Hawaii are secure and tamper-proof.

IDENTITY THEFT CARE KIT

The Identity Theft Care Kit is designed to provide you with information, checklist, worksheet, sample letters and the forms you'll need if you become a victim of identity theft. To receive your free kit, visit us online at boh.com; call Bankoh by Phone at 1-888-643-3888; or request one at a branch nearest you.

BANKOH BY PHONE

If you feel you are a victim of identity theft affecting one or more of your Bank of Hawaii accounts, you can speak to a customer representative 24 hours a day, 7 days a week by calling Bankoh by Phone at 1-888-643-3888 from anywhere in Hawaii, US Mainland or Canada.

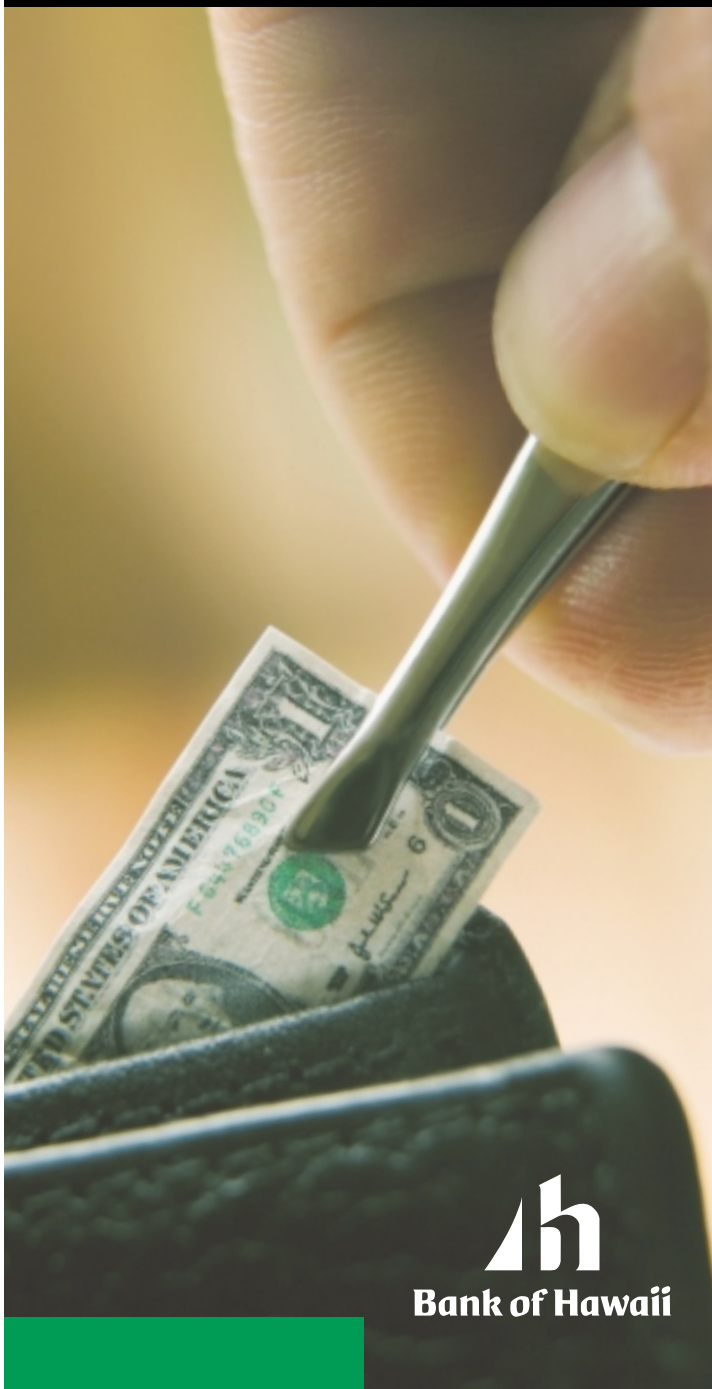
If you would like more information about identity theft, visit us at www.boh.com/idtheft.

Bank of Hawaii

Member FDIC boh.com AD-755 (9/2006)

Protect Yourself

Identity Theft and Safe Practices Guide



Bank of Hawaii

Someone you know is a Victim of Identity Theft

Mention 'identity theft' to an acquaintance and you'll likely hear a story of how someone had their bank check, credit card, debit card or mail stolen.

Victims of identity theft can spend months or years cleaning up the mess thieves have made of their good name and credit record. They may lose job opportunities, be refused loans, education, housing or cars, and sometimes even get arrested for crimes they didn't commit.

You can minimize the risk of identity theft by increasing your awareness, understanding the warning signs, and being cautious and diligent in your efforts to protect your personal and financial information.

Identity Theft Frauds & Scams

More information about identity theft frauds and scams are available online at boh.com.

PHISHING (PRONOUNCED 'FISHING')

Phishing is an internet scam that uses e-mail messages to trick you into visiting a website in order to obtain financial and other sensitive information.

These e-mails pretend to be from a business, such as a store, bank, or credit card company. They often direct you to "update" or "validate" your account information via a fraudulent website that looks similar to (or exactly like) the legitimate business.

ADVANCE FEE FRAUD

E-mail or letters that promise a large amount of money for a nominal (advance) fee are examples of advance fee fraud. They often sound too good to be true and could also include a request for your bank account number.

Typical types of advance fee fraud include:

- Faked internet sale offer for goods or services
- Request for assistance in the transfer of money
- Transfer of funds from over-invoiced contracts
- Disbursement of money from wills to benefactors
- Foreign lotteries

CON ARTISTS

"Con artists" are trained to win your trust in order to extract important information about you, your job, your home, and even your family. The information they obtain is then used to commit fraudulent acts.

Be on the alert if a caller tells you any of the following things:

- You must "act now" or the offer won't be good.
- You've won a "free" gift, vacation or prize, but you have to pay for "postage and handling" or other charges.
- You must send money, give a credit card or bank account number, or have a check picked up by courier. (You may hear this before you have had a chance to consider the offer carefully.)
- You don't need to check out the company with anyone else before responding to the caller's offer.
- You don't need any written information about their company or their references.
- You can't afford to miss this "high-profit, no-risk" offer.

If you hear these – or similar – lines from a telephone salesperson, just say "No, thank you" and hang up the phone.

WARNING SIGNS

The following are some of the warning signs that your identity may be compromised:

- You find unexplained charges or withdrawals on your bank account or credit card statements.
- Your monthly bills or credit card and bank statements suddenly stop arriving.
- You are turned down for a credit card, loan, mortgage, or other form of credit for no apparent reason.
- Your credit report contains inquiries or information about accounts that you didn't open.
- Credit collection agencies try to collect on credit card or loan payments that do not belong to you.
- You start getting bills you do not recognize for goods or services you didn't buy.
- You receive credit cards for which you did not apply.

WHAT TO DO IF YOU BECOME A VICTIM

- Act quickly
- Contact and file a report with any one of the three major credit bureaus
- Call the police and file a report
- Contact your bank and close your at-risk accounts
- Contact the creditors of accounts that may have been fraudulently accessed or opened
- Follow up all contacts in writing and provide necessary documentation such as copies of police reports and FTC ID Theft Affidavits
- Obtain a free copy of your credit report from all three major credit bureaus
- Contest bills that result from identity theft

What you can do to Protect Yourself

- When asked, never give out personal information over the phone, Internet, or by mail.
- Before you volunteer sensitive personal or financial information, confirm the person or organization receiving the information is reliable.
- If you receive unsolicited e-mail that asks you, either directly or through a website, for personal or financial information, exercise extreme caution even if it appears to come from a trusted company.
- When away from home, carry only the identification, credit and debit cards you need. Do not carry your Social Security card or any item bearing that number with you.
- Memorize or keep automatic teller machine PINs (Personal Identification Numbers) in a safe area away from your wallet, ATM card, check card, or checkbook.
- Choose "strong" internet passwords that cannot be easily guessed. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number, etc.
- Install anti-virus, anti-spyware, and a personal firewall on your home computer and keep them updated.
- Find a safe place to store personal information, used and unused checks, credit cards and bank records in your home.
- Dispose of your trash carefully. Shred personal and financial documents before throwing them out or recycling them.
- Install a USPS approved lockable mail box or promptly remove mail after it arrives. Deposit outgoing mail in post office collection boxes or at your local post office.
- Follow up with creditors if your bills don't arrive on time. Review your bills and statements promptly and contact a company immediately if you discover any unexplained activity.
- Obtain a free copy of your credit report once a year by contacting the Annual Credit Report Request Service at 1-877-322-8228 or online at www.annualcreditreport.com.
- Carefully examine your credit report and follow up on discrepancies such as unexplained accounts, incorrect balances and typos.
- Ask the credit reporting agencies about their fraud alert protection programs.