

Identity Theft

Presented by:

Gina M. Barry, Esq.

Todd C. Ratner, Esq.

Jason Shrock,
Business Banking Officer

What is Identity Theft?

Identity theft occurs when someone uses your personal information without your permission to commit fraud or theft.

Identity Theft Statistics

- Since 1999, millions of complaints have been filed regarding Identity Theft.
- 1 in 23 people will become a victim of Identity Theft.
- Identity Theft victims spend from 3 to 5,840 hours repairing the damage done by an identity thief.
- 70% of victims have trouble getting rid of, or never get rid of, negative information in their records.
- 400,000 children under the age of 18 become victims of Identity Theft each year.

**Have you protected yourself
from Identity Theft?**

Self-Test

1. I receive my mail through a mail slot or in a locked mail receptacle.
2. I always deposit my outgoing mail in a post office collection box.
3. In my wallet or purse, I carry no more than two credit cards.
4. I keep a copy of the front and back of the credit cards I carry in my wallet or purse.
5. My Driver's License number is an "S" number, and not my Social Security number.

Self-Test

6. I pay my bills via an electronic funds transfer whenever possible instead of mailing a check.
7. Whenever I must pay a bill by mailing a check, I always write the check using a pen with ink that cannot be washed off of the check.
8. When I must send personal information through the mail, I always send said mail via a traceable means.
9. I shred all documents containing personal information prior to discarding the documents.

Self-Test

10. I never provide personal information to any person or company unless I know how it will be used.
11. I never give out personal information over the telephone or internet unless I initiated the contact.
12. I know exactly how many credit cards I have, and I have placed the cards in a secure location.
13. I maintain a record of the billing cycles for all of my expected bills.

Self-Test

14. Each time I receive a credit card bill, I match my receipts to the transactions listed on the bill.
15. I have removed my name from the pre-approved credit card offers list.
16. I request my credit report from all three credit reporting agencies at least once each year.
17. I actually review my credit reports upon receipt.

Self-Test

18. Whenever third parties are working in or around my home or office, I keep all of my personal information in a locked room or safe.
19. I change the passwords and personal identification numbers ("PINs") on all of my accounts at least every six (6) months.
20. When selecting passwords or PINs, I never use easily obtained information or consecutive numbers.

Self-Test

21. I immediately respond to any notifications I receive regarding possible theft of my personal information.
22. I immediately report any attempts by a third party to obtain my personal information to the proper authorities.
23. I know how to place a fraud alert and a credit freeze on my personal credit file.
24. I am currently enrolled in a credit protection program.

How many times did you
answer "TRUE" on the
Self-Test?

How Identity Thieves Get Your Information

Old-Fashion Stealing

- They steal your incoming or outgoing mail.
- They steal wallets and purses.
- They steal information from documents that are not safeguarded in your home.
- They steal information from their employers or pay unscrupulous employees to steal the information for them.

Dumpster Diving

- Identity thieves rummage through your trash looking for bills or other papers that contain your personal information.

Phishing

- Identity thieves, pretending to be financial institutions or other companies, send e-mail or call you on the telephone and ask you to reveal or verify your personal information.

Sample Phishing E-mail

- **From:** Key Bank Alerts [mailto:provisor67@key.com]
Sent: Wednesday, October 15, 2008 8:44 AM
To: Gina M. Barry
Subject: Key Bank The safest passwords are those that combine numbers, letters and special characters
- **KEY BANK ALERT SYSTEM!** Updates available:
When you bank online with us, your information is encrypted. Encryption makes information unreadable in order to protect it from unauthorized viewing or use, especially during transmission.

[Update your system now>>](#)

For your security and ours, Key employs a robust industry standard for all encryption.

Sincerely, Tami Battle.

Copyright 1998-2008, KeyCorp. All rights reserved.

•

Sample Phishing E-mail

- Dear Banknorth valued member,

On the date of 30th December there was a login trials from a foreign IP address which resulted with your account temporary suspension .

- for your security
- you have to immediately reactivate your account
- Please click reactivate now to reactivate your account
- Sincerely,
Banknorth Security Department
- This notification expires in 48 Hours
Reactivate Now*

Sample Phishing E-mail

- **From:** Wells Fargo Online Banking [mailto:online.security@online-wellsfargo.com]
Sent: Friday, May 02, 2008 1:10 AM
To: Gina M. Barry
Subject: Wells Fargo : You Have 1 Alert Message About Your Internet Banking
- Dear Valued Customer
- Your privacy is a top priority for us at Wells Fargo Bank. Each year, we send our customers a copy of our Privacy Policy so that you know how we collect, use and protect your personal information. This year, we've revised our policy to make it simpler and easy way to understand.
- We've designed our service to ensure that all our customers are assured and protected. To this notification, your online banking facilitations have to be updated to enable us serve you better. **Sign In** to start the validation process:
- Sincerely,
- Privacy Department.
Wells Fargo Online Banking.

Sample Phishing E-mail

From: Woodforest Bank [mailto:customer-service@woodforest.com]

Sent: Tuesday, February 19, 2008 6:35 PM

To: Gina M. Barry

Subject: Online Banking Precaution Against Unauthorized!

- **Dear Valued Customer**

- Woodforest Bank takes significant steps to protect the security and privacy of your information online. We employ best practices to ensure the integrity of our systems and the security of your information. We use several levels of security techniques that consist of prevention, detection and response as well as monitoring and reporting. To further protect against unauthorized access to your accounts, our systems are designed to automatically terminate a secure online session if extended inactivity is detected. If your session is terminated, you will be required to login again to continue. In addition, when you log out, we have taken steps to ensure that the history of your session is not retained. This helps to ensure that your privacy is protected, particularly when using a publicly accessible computer. For your protection, we require that you "VERIFY" your account details. If you are unable to provide either the correct Username or password, you will not be granted access.

- To Verify your details use the reference link below:

<http://www.online.woodforest.com/wnb/>

Pretexting

- Identity thieves pretend to be a
an account representative,
landlord, employer or
governmental entity in order to
obtain your personal information
from third parties.

Imagine receiving this phone call . . .

Skimming

- Identity thieves pay employees of reputable businesses to steal credit and debit card numbers by using a special storage device when processing your card.

Schemes Yet to Be Discovered

- Identity thieves continue to develop new methods of obtaining your personal information for their fraudulent purposes.

Once they have your
personal information,
identity thieves use the
information
in a variety of ways.

Credit Card Fraud

- An identity thief often opens credit accounts in your name, charges numerous or large purchases on these accounts and never pays the bill.
- When an identity thief obtains access to an existing account, the thief will usually change the billing address so that you no longer receive the bill and thus remain unaware of the theft.