BALANCE
Financially Empowering You

Identity Theft Podcast

[Music plays]

Nikki:

You're listening to 'Identity theft protection'. Hi. I'm Nikki, your host for today's podcast. Identity theft occurs when someone uses your name, social security number, credit card number or other identifying data to commit fraud or other crimes.

Fortunately, there are things you can do to reduce the chance of this happening to you and minimize damage if you do become a victim. This podcast covers the basics, including common practices of identity thieves, preventing identity theft, how to recover from identity theft and federal laws.

Common practices of identity thieves. There are many ways identity thieves can illegally access your personal information. Some of these include stealing mail from your mailbox, rerouting your mail to another location by filling out a change of address form, searching your trash or recycling bin, stealing your wallet, smart phone or PDA, misrepresenting themselves to a company that has access to your information.

Hacking into your computer or the computer of a company that does business with you, accessing the information you enter online or send by email, posing as a legitimate company or government agency and requesting your information via phone, which is called phishing, via email, which is called phishing or via text message, which is called smishing, attaching a skimmer to an ATM to capture the card number and PIN and taking advantage of a personal relationship with you.

Once your personal information has been acquired, it can be used in a variety of illegal ways. Common practices include using your credit card. Though some retailers check your ID when you pay with plastic, it's not often done. All a thief needs to do is forge your signature to make an illegal transaction. This is even easier when making telephone or online purchases.

Opening a new credit card account or taking out a loan to buy a car or other expensive item is also common. Unfortunately, you may not even find out about the crime until you experience some type of negative credit or collection action on an account you never opened.

Thieves may also illegally access your checking account. They may write bad checks or use your debit card. Even if they don't have your PIN, they can still make purchases in a store by choosing the credit option or by shopping online or over the phone. Finally, they can obtain government benefits like social security or food stamps or use your health insurance to pay for medical care.

Preventing identity theft. There are steps you can take to reduce the threat of identity theft. First, you should check your credit reports for fraudulent activity at least annually. You can receive a free copy of your reports from each credit bureau, Equifax, Experian and TransUnion once a year by visiting annualcreditreport.com.

If you believe you're a victim of identity theft, you can receive additional free reports by contacting the agencies directly. When you receive your reports, review them for errors or suspicious activity. If you find inaccurate information, contact the bureaus immediately as well as the involved creditors.

Another step to take to reduce the chance of identity theft is to guard your personal information. You should only provide personal data when you're sure the person or company is legitimate and you're the one who initiated contact. You should also know how the information will be used.

Be sure to always check your statements for credit cards, utilities, bank accounts and other accounts when they are issued. If you see unauthorized charges, contact the company immediately. Also contact them if you don't receive your statement on time.

Always protect your mail. Empty your mailbox promptly and sign up for electronic statements whenever available. This will reduce the amount of mail you receive containing sensitive information. Avoid a false sense of security. Never leave your wallet, statements or portable electronic devices out in plain sight. Keep in mind that many people are victimized by someone they know and in familiar surroundings.

Only carry with you what you need. Most people don't need to carry around their social security card and checkbook every day. If your wallet or bag is stolen or misplaced, there will be less sensitive information at risk of theft if some things are left at home. Always shred your statements and other sensitive documents before throwing them in the trash. This also goes for pre-approval offers.

Use a firewall and antivirus and spyware software to protect your computer from hackers. Make sure all your passwords are hard to guess, and always log off your computer when you leave the

room. Don't leave portable devices like laptops, tablets or smartphones unattended. Before selling or disposing of any electronic device, be sure to delete personal information using a wipe utility program.

When shopping online, use a secure browser. Look for the lock icon on the browser status bar and ensure that the URL reads HTTPS and not simply HTTP. Avoid sending sensitive personal information via email, downloading files or opening links sent by people you don't know.

If you're really concerned about the possibility of identity theft, you may consider buying credit monitoring or identity theft insurance. If this is the case, do so only after carefully reading the fine print and weighing the costs against the benefits. Keep in mind that some of the businesses that offer these services are scams themselves. Research the company's history and check the Better Business Bureau's complaint log before signing up.

How to recover from identity theft. If you become a victim of identity theft, being proactive can minimize its impact on you. You may need to communicate with several parties, including creditors and financial institutions. If a credit card or financial account has been used or opened illegally, contact your creditor or financial institution immediately. If the account is not yours, close it. If it is yours, request a new account number and card. Continue to monitor all future account statements carefully.

Legal and government agencies. You may want to file a police report. If you do, request a copy of the report. A credit bureau or creditor may ask you to provide one as part of their investigation. You can also file a complaint with the Federal Trade Commission, although they do not assist with individual cases. In addition, you can contact the US Postal Inspection Service if your mail was stolen or your address was used fraudulently.

Credit reporting bureaus. Check your credit reports from all three bureaus. Remember you're entitled to additional free reports if you believe you are the victim of identity theft. Dispute any fraudulent items. This can be done by submitting a form online or mailing a letter to the credit bureaus.

Even if the fraudulent information hasn't yet appeared on your reports, contact the credit bureaus and have a fraud alert placed on your credit reports. This will require creditors to verify your

identity before opening a new account. This alert only lasts 90 days, but if you file a police report, you can extend the alert to seven years.

If you feel an alert will not provide enough protection, you may want to place a security freeze on your credit report. When a freeze is placed on your report, no creditor or other business that does not have a pre-existing relationship with you can view your report. If you want to apply for credit yourself, you can have the freeze lifted either temporarily or permanently.

There are many federal laws that help in the fight against identity theft. The Fair Credit Reporting Act states that if you're denied credit, insurance or employment because of your credit report, you may get a free report from the bureau that supplied it within 60 days. You have a right to dispute any inaccuracies in your report, and the credit bureaus must investigate the validity of the disputed items within 30 days.

Derogatory information that is outdated or unverifiable cannot be reported, and only those with the need recognized by the Fair Credit Reporting Act may access your file. The Fair and Accurate Credit Transactions Act states that you may receive a free copy of your credit report from each of the three credit bureaus once a year. In addition, you may receive additional free reports if identity theft is suspected.

You may block fraudulent information from appearing on your credit report. You have a right to access business records that document an identity thief's fraudulent transactions. You have a right to place a fraud alert on your credit report if you believe you have been the victim of identity theft. Active duty military personnel may place a special alert on their files when they are deployed overseas.

No more than five digits of a credit card number may be listed on store receipts. The card's expiration date cannot be listed either. Creditors must implement identity theft prevention programs. Debt collectors must inform a creditor of fraudulent information. The Fair Credit Billing Act states that liability for a lost or stolen credit card is limited to $50 if you notify the card issuer within 30 days.

If there has been an error in a credit card bill, the lender must correct it or explain why the amount is believed correct within 90 days after being notified. The Electronic Fund Transfer Act states that you have 60 days to dispute an error involving an electronic fund transfer such as direct deposit and

withdrawal and debit card purchases. The financial institution must respond within 45 days. Any disputed funds must be put back into your account within 10 business days.

In addition, the maximum liability for a lost or stolen debit card or ATM card is $50 if you report it within two business days of noticing the card is lost or stolen, $500 if you report it after two business days but within sixty or no limit if you wait more than 60 days. In other words, you can lose all of the money in your account plus, if applicable, your maximum overdraft line of credit.

If a creditor or credit bureau violates one of these laws, you can submit a complaint with your state's attorney general's office and the Federal Trade Commission.

Violations involving a checking or savings account can be reported to the office of the comptroller of the currency for national banks, the Federal Reserve Board for state banks that report to them, the Federal Deposit Insurance Corporation for other banks, the National Credit Union Administration for federal credit unions and the state financial supervisory board for state credit unions. That's all for this podcast. For Balance, this is Nikki saying thank you for listening.

[END OF TRANSCRIPTION]

Revised 0118