DOWNEASTER COMMON SENSE GUIDE

Gone Phishing

IDENTIFYING AND AVOIDING CONSUMER SCAMS

STATE OF MAINE
BUREAU OF CONSUMER CREDIT PROTECTION
DEPT. OF PROFESSIONAL AND FINANCIAL REGULATION

Maine Bureau of Consumer Credit Protection

Toll-free Maine Consumer Assistance
1-800-332-8529 (1-800-DEBT-LAW)
TTY users call Maine relay 711

Maine Foreclosure Prevention Hotline
1-888-NO-4-CLŌZ
(1-888-664-2569)

www.Credit.Maine.gov

The Maine Bureau of Consumer Credit Protection was established in 1975 to enforce a wide variety of consumer financial protection laws, including:

-Consumer Credit Code
-Truth-in-Lending Act
-Fair Credit Billing Act
-Truth-in-Leasing Act
-Fair Credit Reporting Act
-Fair Debt Collection Practices Act
-"Plain Language" Contract Law

The Bureau conducts periodic examinations of creditors to determine compliance with these laws; responds to consumer complaints and inquiries; and operates the state's foreclosure prevention hotline and housing counselor referral program. The Bureau also conducts educational seminars and provides speakers to advise consumers and creditors of their legal rights and responsibilities.

William N. Lund
Superintendent
July 2014

DOWNEASTER COMMON SENSE GUIDE: GONE PHISHING
IDENTIFYING AND AVOIDING CONSUMER SCAMS

By David Leach, MPA and Steven Lemieux, MBA
Cover Design: Edward Myslik

Maine residents can obtain additional free copies of this booklet by contacting the Bureau of Consumer Credit Protection at 207-624-8527 or toll-free at 1-800-332-8529. Non-Maine residents may purchase the publication for $6 per copy, or at a volume discount of $4 per copy on orders of 50 or more. Shipping fees are included in the prices listed.

Dear Maine Consumers,

In Greek mythology, Eurystheus, King of Tiryns, sent the hero Hercules to slay the Lernaean Hydra — a 9-headed serpent. Each time Hercules lopped off one of the Hydra's heads, two new heads grew back in its place. How Hercules felt when the hydra's heads grew back is how members of our agency staff often feel when consumers ask, "Why can't you shut down all of these scams?"

Criminals frequently use prepaid "burner" phones to avoid being tracked and identified by law enforcement. The few scammers who are caught are usually sent to prison. Unfortunately, there are always others ready to take their place — waiting to separate you from your money.

Government agencies at both the state and federal levels stand ready to assist you if you become aware of a scam, are in the process of being victimized, or have been "taken." The best way to protect yourself is to become a savvy consumer — smarter than the criminals after your hard-earned money, and able to detect scams from a mile way.

This guide is all about helping you defend yourself against being scammed. In the following pages, we describe tactics and hooks used by scammers, offer advice on how to protect yourself, and, if you've already been victimized, how to report the scam to the proper authorities. Take ownership of this multi-billion dollar rip-off and slash the amount of money lost to scams in the United States by becoming the first line of defense — hanging up, saying "No," shredding phony direct mail offers, and deleting questionable, unsolicited emails.

We hope you enjoy the material presented in this State of Maine publication. If you know of other Mainers who could benefit from reading this book, call our office (1-800-332-8529) — we'll be pleased to send additional, free copies to you or to family members, friends or co-workers living in Maine. Remember, knowledge is power!

David Leach, MPA
Bureau of Consumer Credit Protection

Steven Lemieux, MBA
Bureau of Consumer Credit Protection

Cheat Sheet — Identifying Scams

For your convenience, here is a summary of the most common red-flags to help you identify scams:

- **Unsolicited Contact:** If you receive a phone call, e-mail, fax or advertisement from a person or company you're not familiar with, be wary – many scammers use unsolicited messages to find victims.
- **Incomprehensible Investments:** Before agreeing to anything, make sure that you understand what's being offered – scammers will use your confusion to make themselves sound like experts. Ask questions and, if you need to, ask someone you can trust for help.
- **"Act Now!":** Scammers want you to act fast, before you have a chance to think or ask others for advice. Don't be pressured into making a quick decision.
- **Suspicious Payment Methods:** Many scammers ask for money to be sent via unstoppable or difficult-to-trace methods (e.g., wire transfer). Before sending money to a person or business you aren't familiar with, ask yourself "Why won't they let me use a different payment method?"
- **Paying Money to Get Money:** Many scammers ask victims to pay fees for "administrative costs" or "taxes" in exchange for a much larger sum of money. Never pay money to get money – it's a hallmark of financial scams.
- **"Deal of a Lifetime":** Watch out for promises of high returns with little or no risk. There's no such thing as a free lunch – without risk, there is no reward.
- **"Trust Me":** Scammers often ask potential victims to wire money or reveal personal information based on trust. Always ask yourself, "Do I really know who this is? Why should I trust an unsolicited offer from a stranger?"
- **"Tell No One About This Deal":** Many victims report that scammers instructed them to keep a potential "deal" secret. Trust your family and friends – the more people you tell about the pitch, the greater the chance that someone will be able to determine whether or not it's a scam.

Take a deep breath, pause, and ask questions — don't act impulsively! Guard your personal information (date of birth, street or mailing addresses, Social Security number and bank account numbers) – especially during initial calls. Ask for the caller's full name, email address, the official name of the company (as registered with the Maine Secretary of State's Corporation Division), the company's physical and mailing addresses, as well as their State of Maine license or registration number. If they refuse, don't do business with them! If they comply, call the appropriate government agency (see pg. 31) to determine if the business and their sales pitch are legitimate.

Table of Contents

The Art of Persuasion

Consumers fall prey to scammers for a variety of reasons. Sometimes it's a matter of timing – perhaps the victim was going through a rough patch and the call or email arrived at the right moment. Others respond to seemingly legitimate opportunities, or genuinely want to help a person in need. Most scams don't succeed because the victims are gullible – they succeed because the scammers are organized, practiced and ruthless. They know what to say to get you to act.

For a scam to be successful, it needs willing victims! If a consumer isn't willing to participate, there's little that a scammer can do to force them. There are several ways that a scammer may convince a victim to participate:

- **Trust**: Most scams don't rely on a victim trusting the scammer, they rely on the scammer placing trust in a victim. If someone shows trust in you, you are more likely to trust them — and more likely to take risks when dealing with them.
- **Likeability**: You're more likely to do something for someone you like than for someone you don't. Because of that, scammers often put on friendly faces and treat victims as confidants — don't expect them to look or act like criminals until it's too late.
- **Reciprocation**: If someone does something for you, you're more likely to do something for them. Scammers will sometimes give gifts or make offers in exchange for something from a victim.
- **Rarity**: The desire for something rare can be a powerful impulse. Scammers often claim that an offer or deal will no longer be available if the victim doesn't act immediately.
- **Proof**: Testimonials from other consumers who have "profited" from participation in a scam may put a victim's mind at ease before they decide to hand over money. Such endorsements are usually fictional, coming from individuals who are in on the scam.
- **Authority**: Scammers want victims to act without thinking. It's much easier for a con artist to get a victim to act if the scammer appears to have expertise or credentials, or appears to be employed by a legitimate organization or government agency.

"Trust not too much to appearances."

-Virgil (37 B.C.)

The Working Tools of Scammers

Unfortunately, there is no way to completely protect yourself from scammers. However, it pays to be informed — knowledge is your best defense. By familiarizing yourself with the tools and techniques presented here, you'll be well on your way to becoming an expert scam detector.

Phishing

One of the most common tricks in the scammer's playbook is **phishing** — the act of impersonating a person or business in order to trick victims into revealing private information. Phishing scams are usually encountered via email, although **vishing** (phishing scams committed by telephone) and **smishing** (phishing scams committed by text message) are becoming common as well.

Phishing e-mails are often designed to mimic messages from real companies you *might* have an account with. They are usually highly polished, including graphics and language meant to convince you that the communication is legitimate. There are, however, some red flags to help you identify fraudulent phishing messages:

- **Spelling:** If words are misspelled, be suspicious. Phishing messages sent from outside the U.S. frequently contain misspellings and grammatical errors.
- **Hidden Sender**: If the sender's e-mail address is hidden, don't trust the message. (Tip: A hidden e-mail address may be revealed by hitting "reply all.")
- **Date Format**: If a message from an American company contains dates, be sure that the date begins with the month. If the date begins with the day, the e-mail may be from outside of the country — a tipoff if the company says it is located in the United States.
- **Generic Greetings:** Most legitimate companies address consumers by name in email messages. If a message has a generic greeting such as "Dear Customer," there's a good chance that it's a phishing scam.
  - While most scammers send out generic messages, some may research you in order to gain your trust. Beware these so-called "**spear phishing**" scams.
- **Requests for Personal Information**: If an unsolicited email requests personal information, it's probably a phishing scam.

Were You Aware?

If a phishing scam targets a CEO or business person, it's called "whaling."

- **Email Address:** Many phishing e-mails come from accounts chosen to mimic those of legitimate companies (i.e. "Alerts@XYZ.co.uk" vs "Service@XYZ.com"). Be sure that the email address which sent the message matches company the email is "from."

- **Forged Links**: Just because an email link contains a name you recognize doesn't mean that it links to a real company. Move your mouse over the link to reveal where it is directed to, and see if it matches up with the email address of the sender. If they don't match, don't click on the link.

  - If you follow a link, watch out! Although you may be sent to a website with pictures and branding from a real company, the page could be a well-made fake.

If you receive a phishing email, beware of attachments. Some phishing scammers attach malicious software (**malware**), such as viruses or **spyware** (software that gathers information from your computer without your knowledge), which activates when the attachment is opened.

High Pressure Tactics

A hallmark of many financial scams, **high pressure tactics** are designed to make you act before you think. There are lots of different ways for a scammer to put pressure on you, but they all have one thing in common: they push you to act *NOW*. In some scams, the criminal will claim to offer a special discount on a product or service but for a *very* limited amount of time. They may threaten to take you to court or have you arrested unless you do what they want immediately, or warn you that if you don't take action something bad will happen.

If someone you don't know wants you to do something immediately, stop, take a deep breath and remember these guidelines:

- **Identify the Company**: Make sure you know who's calling. If you weren't given or don't remember the caller's name, company and/or product, ask for it and write it down in case you want to submit a complaint later. If the caller won't identify themselves, hang up.

- **Command the Conversation**: Remember, they called you and are taking up your time. Don't be afraid to ask questions and don't be intimidated. Be assertive!

- **Stop Them Early**: The longer a call persists, the harder it is to end. If the caller raises their voice, has an arrogant tone, or doesn't seem to care that you're not interested, find a way to end the conversation or simply hang up.

- **Be Cautious**: Ask for written descriptions of services, charges and refund policies. Don't be pressured into providing information like addresses, Social Security numbers, date of birth, credit card information or bank account numbers.

- **Trust Your Gut**: If something feels wrong, it probably is — end the call as soon as possible.

Funds Transfers

Electronic funds transfers (EFTs) are exchanges or transfers of money through computer-based systems. EFTs, particularly **wire transfers**, are quick, easy ways to send cash - as such, they're a favorite tool of scam artists. Because wire transfers move fast and are difficult to reverse, scammers often ask consumers to use them as payment methods — taking the money, making an untraceable cash deposit at their bank and disappearing before their victim realizes what has happened. If money has been sent to a scammer via wire transfer, it's nearly impossible to recover.

To protect yourself from scams using wire transfers and other types of funds transfers:

- **Beware of High Pressure Tactics**: See pg. 2.

- **Know Who You're Sending Money To**: Never send money to someone that you don't know — even if they try to entice you with deals, sales, work offers, or claims that you've won a prize. If someone who says they know you asks you to send money, confirm it in person or through a separate (known) phone number or e-mail address.

A Note About Wired Funds

A reoccurring theme in this guide is to be wary of high-pressure marketers and solicitors pitching "too-good-to-be-true" offers and demanding wired funds. The money-transmitting industry, which allows consumers to wire funds from supermarkets, department stores, and drug stores to a friend or relative in a far-away place, provides a great service. Companies like Western Union, Money Gram and Green Dot do a good job of warning consumers to not fall prey to scammers asking for wired funds at their retail transmitting locations. It's not the service that's at issue, it's the occasional reckless use by customers.

Ultimately, each of us must make the final decision on whether to wire funds as a result of a solicitation for goods or services. Most legitimate businesses will accept credit or debit cards, with the issuing bank ready to step in to help you if there is a dispute or fraudulent transaction.

- **Don't Accept Overpayments**: If you're selling an item never accept an overpayment, especially is the sender asks you to send the excess back by wire transfer — it may be a **fake check scam** (pg. 13).

- **Chose a Different Payment Method**: If you do decide to send money to someone you don't know, retain control by using a check with a stop-payment feature.

Spoofing and VOIP

Many phones are equipped with Caller ID, a service which displays the phone number and/ or name of a caller (sometimes offered as an optional service for an additional fee). Caller ID is a useful tool for screening calls, but it can't always be trusted. It's possible to "spoof" telephone numbers and names – making the calls appear to be from individuals or companies other than the actual callers. Crooks seeking consumers' personal information often use Caller ID to hide their identities, making it appear that they are calling from the government, a bank, or another organization.

Voice Over Internet Protocol (VOIP) – Internet phone, texting and fax services are also popular methods used by scammers to conceal their identities. Unlike spoofing, where the caller disguises themselves by faking their caller ID, VOIP scams use internet phone numbers which have been set up with legitimate-sounding names.

Fake Feds

A call or email from a government agency is sure to get anyone's attention. Because of that, many scammers disguise themselves by using the names of well known federal agencies (e.g., FBI, IRS, Federal Reserve Board), or by making up names that sound government-like (e.g., "State National Credit Investigation Bureau").

Government agencies rarely, if ever, make initial contact with consumers by e-mail — it's too difficult to determine who an email address belongs to. If you receive an unexpected e-mail from a government agency, it's probably a fake. If you receive a call out of the blue from someone claiming to represent a government agency, take down their information (name, phone number, etc.) and do some research. Contact the agency they claim to work for to determine if the call was legitimate. If you've encountered fake feds, consider filing a complaint with the U.S. Secret Service.

Mass Marketing

Mass marketing is encountered every day through e-mail, websites, television, radio, phone and mail — it's a useful tool for companies trying to reach out to consumers. Unfortunately, scammers use mass marketing as well. No matter the medium, mass

marketing scams have two main components — they are an attempt to rip off lots of people at once with minimal effort, and they depend on victims giving money in exchange for promises of goods or services which the scammers will not deliver.

Two types of mass marketing scams merit special mention. The first is **spam**, unsolicited e-mails sent out in the billions. These messages may be sent via a single individual, a group of spammers, or botnets (aka "zombie networks") — networks of computers infected by malware. Botnets are incredibly efficient at sending spam. Pitcairn Island in the South Pacific, with a population of roughly 50 people, is estimated to be the source of more than 10,000 spam e-mails per year due to malware infecting residents' computers.

Got Spam? Forward it to the Federal Trade Commission at **spam@uce.gov**

Robocalls, telephone calls placed by a computerized system delivering pre-recorded messages, also merit special mention. In and of themselves, robocalls are not illegal — many are emergency announcements, political advertisements, or legitimate offers from companies.

One of the most infamous robocall scams is Card Services, featuring a message from a fictional woman named "Rachel." Rachel advises the listener to press a number on the phone's keypad if they're interesting in having their credit card's APR reduced, or a different number if they want the calls to stop.

If you press any number, it tells the automated system that it has reached a live, person. That number is then assigned to an aggressive telemarketer who uses high pressure tactics to get the victim to pay for the company's non-existent "service." Victims often report being bullied into disclosing their Social Security numbers, dates of birth, full names and street addresses — potentially leading to identity theft (See **Identity Theft**, pg. 7, **Debt Relief Scams**, pg. 14).

To protect yourself from mass marketing scams:

- **Watch for Spelling and Grammar Errors**: It's rare that a legitimate company will distribute misspelled or grammatically -incorrect mailings. If you receive such a mailing, be suspicious.

- **Guard Your Information**: Never give out sensitive personal or financial information to unsolicited callers.

- **Beware High-Pressure Tactics**: See pg. 2.

- **Ask For the Offer In Writing**: Interested in what the company has to offer? Ask for information, payment details and terms in

Were You Aware?

"Spam" got its name from a sketch on *Monty Python's Flying Circus*.

writing — legitimate companies will be happy to provide it.

- **Get Detailed Information**: If you talked to someone over the phone, what was their name? Write down the name of the company, the company's street and mailing addresses, and any licenses or registrations that they claim to hold.

- **Research the Company**: Make sure that you know at least a little about the business before agreeing to anything. Do they have a good reputation? Have people complained about them? If so, what were they complaining about?

  - **Astroturfing**: Don't believe everything you read. Astroturfing — posting fake reviews to improve a company's image — is not unheard of online.

It's always a good idea to check with state regulatory agencies before doing business with companies with which you're not familiar. See **Consumer Resources** (pg. 31) for state regulators' contact information.

"Price is what you pay. Value is what you get."

-Warren Buffett

In-Person Scams

Although most of the scams covered in this book are encountered through e-mail, Internet or phone, there's always a chance that you may run into a scammer in person. They might solicit in a public place, or even try to con you at home! To protect yourself from in-person scammers:

- **Take Down Information**: Before agreeing to do business with anyone that solicits you, make sure to write down the business' name, address and phone number, as well as the name of the person with whom you spoke.

- **Check Them Out**: See **Research the Company** (pg. 6).

- **Stop Them before They Start**: It's much easier to stop a sales pitch before it starts than after it has begun. If you're not interested, tell them immediately and hold your ground. Don't be afraid to shut the door on the person.

- **Don't Let Them In**: If someone you don't know has solicited you, **do not** let them into your home. Apart from being potentially dangerous, it can be difficult to get con artists to leave once they've been invited in.

- **Don't Be Pressured**: As with many scams, door-to-door con artists want you to act very quickly, before you have a chance to think about what you're doing. See **High Pressure Tactics**, pg. 2.

Identity Theft

Although identity theft has been around for a long time, it didn't burst onto the scene in a big way until the 1990s – fueled by an increase in remote payment methods (e.g., credit cards) and the relative ease of gathering personal information. Today, identity theft is a big business. According to the U.S. Justice Department, American consumers lose between $18 billion and $34 billion to ID theft each year.

As it applies to personal finance, identity theft comes in two types. The first is **name fraud** — when a crook uses a victim's information to open accounts, request credit cards or apply for loans. The second type is **account takeover** — when a criminal uses a consumer's information to gain access to an account, draining the victim's funds. A thief may obtain information in a number of ways, including:

- **Dumpster Diving**: Searching through trash for discarded credit card statements, cancelled checks, preapproved credit card offers, or other documents containing personal information.
- **Mail Theft**: The illegal interception of mail or other documents.
- **Shoulder Surfing**: Observing a person as they divulge personal information (e.g., watching a person as they enter their PIN at an ATM).
- **Pharming**: Redirecting Internet traffic from a legitimate website to a fake site which asks the victim to provide personal information.
- **Pretexting**: Creating a fake situation that increases the chance a victim will reveal personal information (see **Phishing**, pg. 1).
- **Skimming**: Using a card reader (usually handheld or affixed to the front of an ATM) to capture account information encoded on the magnetic strip of a credit or debit card.
- **Data Breaches**: When a business, government agency or other organization's electronic or written records are stolen or accessed by an unauthorized party.
- **Tombstoning**: Collecting information from cemeteries or obituaries in order to steal identities from the deceased.

Using stolen information, an identity thief can do anything from ordering magazine subscriptions to submitting tax forms and applying for the victim's tax refund. The most common use of stolen information is to fraudulently obtain a credit card.

Unfortunately, most victims don't discover that their identity has been stolen until long after the fact. Some are tipped off when they receive a bill or collection notice for an item or service they didn't purchase, while others discover that they've become victims after receiving notices from financial institutions, being served with legal process, or being denied credit. The best way to protect yourself from identity theft is to prevent criminals from obtaining your information in the first place. To help stamp out ID theft in Maine:

- Never reveal personal or financial information over the phone or Internet unless you initiated contact and are sure of the other party's identity.
- Before sharing information, ask why it's needed, how it will be safeguarded, and what will happen if you don't share it — don't share information unless it's absolutely necessary.
- Lock documents containing sensitive information in a safe place at home
- Shred all documents containing personal or financial information before disposing of them, and don't put your garbage can out overnight.
- Limit the amount of information that you carry with you – remove Social Security cards and any unnecessary forms of identification from your purse or wallet.
- Memorize Social Security numbers and passwords rather than writing them down.
- Watch how much you share online – social networks are powerful tools for criminals searching for personal information.

A Note on Passwords

Passwords can be incredibly valuable to an identity thief, giving them instant access to sensitive information. Be sure to use strong passwords (at least 12 characters) containing a mix of upper and lowercase letters, numbers and symbols. Never share passwords between accounts and never include personal details like names, birthdays or hometowns (that information is easy for an identity thief to find online, weakening your password).

Consider inverting your password, so that instead of something like "Coolguy_50," it reads "Coolguy_5005_yuglooC" – doing so makes a password surprisingly difficult to guess. You could also take a line from your favorite movie or lyrics from your favorite song, string together the first letters of each word and add some numbers. For example, "Only the ghosts in this house are glad we're here 1959" would become "Otgithagwh1959" – not an easy password to crack!

Credit Reports

The most effective way to detect identity theft is to monitor your credit reports. A credit report is a record of your financial history, and contains four types of data:

- **Identifying Information**: Data used to identify you and to differentiate you from other people with the same name, including your address, birthdate, social security number and employment information.

- **Trade Lines**: Information on your credit, including types of accounts and the dates that your accounts were opened, as well as loan amounts, balances, credit limits and payment history.

- **Credit Inquiries**: A list of everyone who has accessed your credit report in the last two years, including voluntary requests (reflecting requests for credit made by you) and involuntary requests (made by lenders issuing pre-approved offers).

- **Public Records and Collections**: Bankruptcies, foreclosures, liens, judgments and other information gathered from courts, as well as information on overdue debts submitted by debt collectors.

It can be time-consuming to review and clean up a credit report, but it's worth the effort. If someone has opened accounts in your name, your credit report will list those accounts. Every consumer is entitled to a free credit report from each of the three major consumer reporting agencies (Transunion, Equifax and Experian) once every twelve months. Request a single credit report every four months, changing agencies each time. When you receive your credit report, look it over carefully. Do you see anything unusual? Keep an eye out for accounts you don't recognize, debts you don't owe, addresses where you've never lived, employers you've never worked for and anything else unusual – these could be simple mistakes, or a sign that your identity has been stolen.

Order Your Free Credit Report

You can safely request a free copy of your credit report by phone, Internet or mail. If you make your request online, have your printer ready. Once you answer a series of personal financial questions to confirm your identity, your credit report(s) will be displayed on the computer screen.

Order by Phone

1-877-322-8228

Order Online

www.AnnualCreditReport.com

Order by Mail

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

(see pg. 29 for a request form)

You have the right to challenge errors or omissions on your credit reports, but that doesn't mean that a credit bureau will automatically make a change if you request one. The agency will conduct an investigation, and you may be required to supply evidence that supports your change request.

If you believe your identity has been stolen:

- Contact your financial institution(s) and place a fraud alert or freeze on any accounts that may be affected. If you disclosed banking information to an unknown caller, **act immediately** — every second counts!

- File a report with law enforcement (local police department, county sheriff, or the Maine State Police). Be sure to keep a copy of the police report — it's important for correcting your credit report and for stopping debt collectors calling about debts you don't owe.

- Place a **fraud alert** on your credit reports to tip off anyone who requests your credit history that you may be a victim of fraud.

- Place **file freezes** on your credit reports. A file freeze locks down your credit report, preventing consumer reporting agencies from releasing your information to a third party without your authorization. If you are a victim of identity theft and have filed a police report, this process is free of charge.

  See pg. 27 for a file freeze form (or contact the Maine Bureau of Consumer Credit Protection at 1-800-332-8529).

- Contact the Federal Trade Commission's Identity Theft Hotline at 1-877-438-4338 (dial "0" to reach a customer service representative).

Pre-Approved Credit Offers

Thieves have been known to steal credit card applications from mail boxes. If you don't want these offers in your mailbox, opt-out!

Call 1-888-5-OPT-OUT
(1-888-567-8688)

The major consumer reporting agencies will remove your name from most credit card marketing lists.

Fraud Alerts

To place a fraud alert, contact Transunion, Equifax or Experian (see below). Report that you've been a victim of identity theft, and ask the company to place the fraud alert on your credit file. No matter which agency you contact, it should forward your request to the other two credit bureaus. Be sure to confirm that this will be done.

Experian	**Equifax Information Services**	**Transunion LLC**
P.O. Box 4500 Allen, TX 75013	P.O. Box 105069 Atlanta, GA 30348-5069	P.O. Box 2000 Chester, PA 19022-2000
1-888-397-3742 www.experian.com/fraud	1-800-525-6285 https://www.ai.equifax.com	1-800-680-7289 https://fraud.transunion.com

Hook, Line and Sinker: Common Scams

419 Scams (aka Nigerian Email)

"I'm a prince/businessman/traveler/soldier, and need your help! While in (country) I managed to get a hold of a large sum of money. Unfortunately, I need a bank account to transfer the money to/cash to pay bribes in order to get the money released/funds to rescue a colleague or family member who is in distress. Would you help me by sending your bank account number/a wire transfer? If you do, I'll give you a large cut of the profit/a reward, far more than the sum(s) you sent me. Can I trust you?"

If this sounds familiar, you've probably already encountered one of the oldest tricks in the book, the 419 scam (referring to the Nigerian Criminal Code article dealing with fraud). 419 scams are double trouble for victims. Not only do these scams pose a financial threat, the scammers often ask for additional information which can be used to steal a consumer's identity. Even scarier, in a few cases scammers have lured consumers to their country — only to cause physical harm to the travelers.

If you responded to a 419 scam, contact your financial institution immediately to close your account, in addition to contacting the FBI or U.S. Secret Service. If you revealed personal information, monitor your credit report closely for unusual activity and consider placing a file freeze, as there is a risk of identity theft.

809 and Missed Call Scams

809 scams rely on area codes set by the North America Number Plan. An **autodialer** (a machine or program that automatically dials phone numbers) rings a consumer's number, leaves a brief message and hangs up, maximizing the chance of a missed call. When consumers look at their caller IDs and call the number back, the trouble begins. Despite the phone number showing the area code, the victim actually calls back on a premium line — being charged up to $30/minute. When the victim receives their phone bill, they may find fraudulent "**cramouflaged**" fees is addition to the exorbitant per-minute billing rate.

What makes consumers call the scammers back? Victims sometimes receive threats of pending litigation asking them to call the number to resolve the issue. If you receive unexpected demanding or threatening communications from another country, think twice about calling back! It can be difficult to reverse charges from telecommunication carriers outside the United States.

Cramouflage: The act of hiding fraudulent charges among real charges — from cram (to fill or stuff) and camouflage (to hide).

To protect yourself from 809 scams, watch out for calls from area codes in the Caribbean, including the Dominican Republic (809, hence the name), the British Virgin Islands (284), Grenada (473), Jamaica (876) and Bermuda (441), among others. Not sure if the call you received is from outside of the U.S.? Visit the North American Number Plan Administration (NANPA) at www.nanpa.com for a list of area codes used by NANP member countries.

Advance Fee Fraud

Advance fee fraud targets consumers with poor credit histories who have been turned down by local banks and credit unions for loans, as well as consumers who need cash beyond what can be provided by personal loans ($1,000-$4,000) and who lack collateral (homes, stocks/bonds, paid-off vehicles, etc.) to pledge as security.

In advance fee fraud scams, a con artist will offer a consumer a loan in exchange for an up-front payment. Although the scammer may assure the victim that the company is located in the United States, the money sent by the victim is often directed out of the country. In addition to causing financial damage, advance fee scammers often ask for personal information which can be used to steal a consumer's identity (see **Identity Theft**, pg. 7).

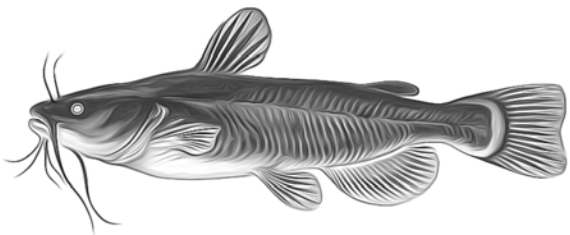
Requesting advance payments in exchange for consumer loans is illegal in both the U.S. and Canada. If you receive *any* offer of credit or a loan and are asked to pay a fee in advance, you are being scammed. If you believe you are a victim of advance fee fraud, file complaints with the Maine Bureau of Consumer Credit Protection and the Federal Trade Commission (FTC). If you wired funds, also report the scam to the money transmitter (e.g., Western Union, Moneygram, GreenDot). In most cases there is little that can be done to recover money lost to advance fee fraud scams; however, filing a complaint may help prevent others from becoming victims.

Catfishing (Dating Scams)

Millions of people flock to dating websites every year looking for love, making these sites attractive hunting grounds for con artists. Online, anyone can be whoever they want to be — the perfect cover for scammers.

Many dating scammers claim to be from the U.S., posing as successful businessmen or contractors traveling or working in another country. Although contact is initially made through a dating site, scammers usual try to move the conversation to e-mail or instant messaging as quickly as possible in case their account is detected and removed.

Eventually the conversations turn to money. The con artist may claim the consumer's banking information is needed, or try to ply the consumer with a sob story — a lost visa, unexpected travel expenses, a medical emergency, etc. If the victim doesn't send



money immediately the tone of the conversation changes drastically. The scammer gets more direct, hounding the victim for what he or she ultimately wants — cash.

U.S. consumers lost more than $55 million to romance scams in 2012. Don't become a statistic. If you met someone online who starts asking for money or financial data, cease communication immediately. If you believe you may be a victim of a dating scam, file complaints with the FTC, the Internet Crime Complaint Center (IC3), and the Maine Attorney General's office. If you gave out sensitive financial information, contact your financial institution immediately and close your accounts (see **Identity Theft**, pg. 7).

Charity Scams

Every year, thousands of well-meaning Americans are scammed out of their hard-earned money by fake charities. Many scam artists take advantage of well-known disasters such as 9/11, the Boston Marathon bombing, the 2010 Haiti earthquake or Hurricane Katrina, tugging at consumers heartstrings and enriching themselves with donations.

You Can't Con an Honest Man

The saying "you can't con an honest man" isn't entirely true. There are many scams that rely on generosity or kindness. However, scammers often rely on making consumers believe they have an unfair advantage over the con artist, tempting victims by offering a windfall at the crook's expense.

The Charitable Solicitations Program at the Maine Office of Professional and Occupational Regulation (1-207-624-8603) requires that most charities operating in the State of Maine be licensed. Be an informed giver — call, check, and verify before giving!

Fake Check Scams

In fake check scams, a consumer receives what appears to be a real check for a large sum. The scammer then requests that a portion of the money be wired back to them as soon as possible (usually as a refund or for payment of "administrative costs" or "foreign taxes"). The victim deposits the phony check and, once they see that the cash is available, wires the requested funds.

Just because money appears to be available after a check is cashed doesn't mean that the check is real — it may take a few weeks for the victim's bank to learn that the deposited check is drawn on a closed or non-existent foreign bank account, leaving the consumer on the hook for both fees and money withdrawn against the check, in addition to the cash sent to the scammer.

To identify fake checks, look for misspellings and thin or low quality paper. To protect yourself from these scams, don't accept payment by check from anyone you don't know. If you do accept a check as payment, ask for a check drawn on a bank with local branches so that you can bring it to the bank to find out if it's real. If you've fallen victim to a fake check scam, contact the Maine Office of the Attorney General and file complaints with

the Federal Trade Commission and U.S. Postal Inspection Service.

Aggressive/Phony Debt Collection

Recently, there has been an uptick in reports of debt collection scams — aggressive, unlicensed debt collectors calling for accounts not owed by the consumer. The callers are relentless. They bombard victims day and night, and aren't shy about calling the victims at work or disclosing information to neighbors, co-workers and supervisors. Common threats used by unlicensed debt collectors include jail, court suits, wage garnishment and disclosure of debt to co-workers, friends, or family members.

The threats are empty. Unfortunately, some consumers wire funds to get the unlicensed collectors to stop calling. While one particular company may stop trying to collect, it often sells the victim's contact information to a new scammer who restarts the process knowing the victim has already succumbed to pressure (paid phony debt).

If you've been contacted by a debt collector and are unsure of whether it's legitimate, write down the name, address and phone number of the collection agency (as well as the name of the person you spoke with). Also ask the collector to provide official documentation of the debt.

Check with the Maine Bureau of Consumer Credit Protection to find out if the collector is licensed to operate in Maine and to ask for advice on how to proceed.

Debt Relief Scams

Many households struggle with repayment of excessive debt, including high credit card balances with excessive interest rates. Legitimate debt management service providers (DMSPs) can provide safe credit counseling options for debtors — helping consumers to obtain debt settlement offers or interest rate (APR) reductions from creditors.

To operate in Maine, DMSPs must be registered with the Bureau of Consumer Credit Protection. Unregistered, fraudulent DMSPs target consumers who are behind on loan payments, and demand up-front fees in exchange for the promise of lower interest rates on credit cards, vehicle loans or personal loan accounts — only to not provide any service. Victims often report sending a few hundred to several thousand dollars to unregistered debt management service providers before reporting the scam.

If the companies are not registered and bonded, state regulators will have a difficult time getting your money back. The Maine Bureau of Consumer Credit Protection's website lists all DMSPs registered by the State of Maine — simply visit www.Credit.Maine.gov, click on "License Types" and select the debt management service provider roster. If the company that is contacting you isn't on the list, hang up! If you've been contacted by an unregistered debt management service provider, contact the Maine Bureau of Consumer Credit Protection. See also **Foreclosure Rescue Scams**, pg. 15.

Foreclosure Rescue Scams

Foreclosure rescue scams hit consumers when they're already down. If a consumer's home is going into foreclosure, scammers may offer to help save the consumer's property, for a price. They falsely guarantee that a loan modification will be obtained or that the foreclosure process will be stopped.

Most foreclosure rescue scammers tell the consumer that they must make up-front payments, or that they must pay the company money to be put into a trust account. Know your rights — a debt management provider is not allowed to charge a customer until it has given them a written offer of relief from their lender, and the customer has accepted that offer. The company must also provide the consumer with documentation showing how the loan will change if the customer accepts the offer, and tell the consumer how much they will be charged for the company's services.

If your home is in danger of foreclosure, call Maine's foreclosure prevention hotline at 1-888-NO-4-CLŌZ (1-888-664-2569) for referral to a free, Maine-based HUD-certified housing counselor. See also **Debt Relief Scams**, pg. 14.

Foreign Exchange Fraud

Foreign exchange fraud is a type of investment scam (see pg. 17) in which a con artist convinces a victim that they can expect a high return by trading currency on the foreign exchange market. Currency exchange trading is a zero-sum game — in order for someone to make money on the foreign exchange market, someone else has to lose money. It's extremely rare for an inexperienced investor to make money on the foreign exchange market.

Before considering investing in foreign currency, consult a financial professional, check with the Maine Office of Securities (1-877-624-8551 | www.investors.maine.gov) to

"Make a habit of two things: to help; or at least to do no harm."

-Hippocrates

Fell for a scam? Watch out for more

If you do fall victim to a scam, watch out. Many scammers participate in **reloading** — scamming victims over and over until they are sucked dry financially. Your name may be added to a **"sucker" list** — a list of people who have been successfully solicited or scammed. They know that if you've been tricked once, they may be able to trick you again.

determine whether the salesperson is licensed to operate in Maine, and check with the Commodity Futures Trading Commission (1-866-366-2382 | www.cftc.gov) for background on the business.

Government Grant Scams

Recently, a consumer received a grant offer from an organization calling itself the "Federal Treasury Department." The senders claimed that in exchange for $200 wired up front, they would send the consumer a "$7,000 U.S. Government grant" within 48 hours. What the scammers didn't realize was that their intended victim was an employee of the federal government, who immediately reported the scam to our agency!

Grant scams are a type of advance fee fraud, with con artists pitching grants in exchange for upfront fees and disappearing as soon as they receive the money. A grant is non-repayable funding given to a person for a particular purpose — often research, higher education, or professional training. Grants, by their nature, are **free**. If you believe that you've fallen victim to a government grant scam, file complaints with the Maine Office of the Attorney General and the Federal Trade Commission. See also **Advance Fee Fraud**, pg. 12.

Imposter Scams

Imposter scams are simple, yet devious. A consumer (usually elderly) will receive a call, text or other message from a con artist who claims to be a friend or relative (often a child or grandchild). The scammer asks for money, claiming to be in some kind of trouble. Occasionally other scammers — impersonating authority figures such as lawyers, police officers or judges — are involved, "validating" the first scammer's story.

One reason that imposter scams are so common is that scammers can pull them off with little or no research. Many of these calls begin with something along the lines of "Guess who this is." Any response gives the scammer an instant identity without having to do any work. Often, the scammer(s) ask questions during their call, tricking the victim into revealing personal information.

If you're contacted by someone claiming to be a friend or family member in an unusual situation who needs a large sum of money, don't give away too much information. Ask their name. If they respond with a generic "it's me" or "your grandson/granddaughter," give them a name that no one in your family has — "Bill," for example. If they confirm that they are "Bill," it's a scam. Alternatively, consider asking questions that only the person claiming

"No death, no doom, no anguish can arouse the surpassing despair which flows from a loss of identity."

-Howard Phillips Lovecraft
Through the Gates of the Silver Key

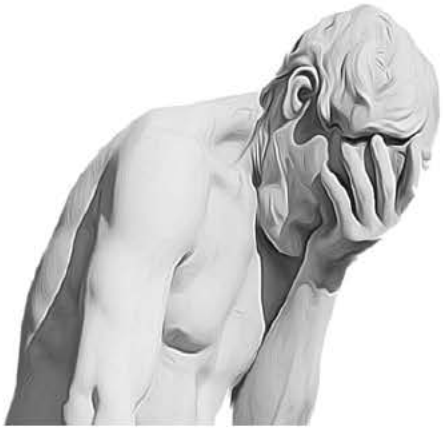
to be on the phone could know, such as "what's your mother's maiden name?" or "what's the name of your pet?" If they're unable to answer correctly, hang up.

If you've fallen victim to or been contacted by someone perpetrating an imposter scam, file complaints with the Maine Office of the Attorney General and the Federal Trade Commission or the Internet Crime Complaint Center (www.ic3.gov). If you provided financial information, contact your financial institution immediately to close your account.

Investment Scams

Imagine that you've received a call from someone offering you an investment opportunity — the formation of a new company or something resulting from an event in the market. They might be vague on the details, but promise a high return on your investment with little or no risk. It sounds like a good deal, right? Not so fast. You may have just encountered an investment scam.

Risk equals return. The higher the return you're expecting, the greater the risk associated with the investment. Be skeptical of anyone claiming differently, and don't be afraid to get a second opinion on investment opportunities before acting. Before committing, ask yourself, "do I really understand the product being offered?" If the caller gets angry or is unwilling to wait for you to get a second opinion, hang up. Scammers want you to act immediately, before you get suspicious.



Before doing business with an investment professional, be sure to check with the Maine Office of Securities (1-877-624-8551| www.investors.maine.gov) to determine whether the person offering the investment is licensed to operate in Maine and what type of services they are able to provide.

If you've fallen victim to an investment scam, file complaints with the Maine Office of Securities. If you gave out personal information, see **Identity Theft,** pg. 7.

IRS Scams

IRS scams have been around for a long time. IRS scammers claim to be Internal Revenue Service (IRS) agents who need immediate access to a consumer's bank account(s) due to fraud or federal tax issues. The rattled consumers give the information to the "agent," who electronically removes money from victim's account.

The real IRS makes initial contact with consumers by mail, will not ask for untraceable or unstoppable payment methods, and will not involve police or other agencies in tax issues. If you think the IRS is trying to contact you, call them directly at 1-800-829-1040.

If you believe you've fallen victim to an IRS scam, contact the U.S. Treasury Inspector General for Tax Administration (1-800-366-4484) and file a complaint with the Federal Trade Commission. In your complaint be sure to note that it is an IRS scam. If you were contacted via e-mail, forward the message to phishing@irs.gov. If you provided personal information, or if the caller knew personal details such as your Social Security number, see **Identity theft**, pg. 7.

Job Scams

Scammers often take out ads in local newspapers or create websites that, for a fee, will "teach you the secrets" of applying for government jobs or offer to link you up with the job of your dreams. These scams are often directed at people interested in finding a job in state or federal government.

Information about U.S. Postal Service, local, state, and federal government jobs is free and available to anyone who's interested. Government agencies never charge application fees, and never guarantee that anyone will be hired for a position — watch out for any ads that claim otherwise. If you believe that you've fallen victim to a job scam, file a complaint with the Maine Office of the Attorney General.

Lottery and Sweepstakes Scams

Lottery scams are a type of advance fee fraud. In lottery scams, a consumer receives an unexpected call, e-mail or letter informing them that they have won a large sum of money in a foreign lottery. The scammer asks the victim to send money for "processing fees" or other charges before the money can be released. There's just one problem — it's not possible to win a lottery without purchasing a ticket! If you haven't purchased a ticket, you can't have won.

There are a number of variations on this scam. Lottery scams can be fronts for aggressive sales pitches. A scammer may claim the consumer has won a free prize (such as a night at a hotel), before pressuring the victim to spend more than the value of what they've "won" on extra goods or services. Sometimes a scammer will claim the victim has won a drawing which didn't require a ticket. Occasionally a scammer

Looking For a Job?

Free, Legitimate Resources

Federal Government

www.USAJobs.gov

U.S. Postal Service

www.USPS.com/Careers

Maine State Government

Bureau of Human Resources
4 State House Station
Augusta, ME 04333-0004

1-207-624-7761
TTY: Call Maine Relay 711
www.Maine.gov/bhr/State_Jobs

Other Maine Jobs

Bureau of Employment Services
55 State House Station
Augusta, ME 04333-0035

1-800-457-8883
TTY: Call Maine Relay 711
www.MaineCareerCenter.com

may offer to purchase tickets in a foreign lottery for the victim.

If you've been contacted about winning or entering a foreign lottery, file complaints with the Maine Attorney General's office and the Federal Trade Commission. If you provided your bank account number or other financial data, contact your financial institution immediately to close your account. See **Identity Theft**, pg. 7, and **Advance Fee Fraud**, pg. 12.

Mystery Shopping Scams

Mystery shoppers are hired by companies in order to evaluate service in retail stores. Most of the time mystery shoppers are instructed to make a purchase at a store or restaurant and report on the quality of their experience. Often the consumer gets to keep the product or service purchased and, in some cases, a small payment as well.

Most legitimate mystery shopping positions are posted online. Avoid responding to mystery shopper advertisements encountered by email or in the newspaper — many of these aren't real. Likewise, never pay for a mystery shopper "certification" (which is often worthless), for access to a directory of companies that hire mystery shoppers, or to be included in such a directory. Above all else, never respond to a mystery shopping opportunity which involves depositing a check or wiring funds in advance (see **Fake Check Scams**, pg. 13).

Mystery shopping can be fun, but it's rarely a gateway to riches. If you think that you've fallen victim to a mystery shopping scam, file complaints with the Maine Office of the Attorney General and the Federal Trade Commission.

Illegal Payday Loans

Payday lenders offer a valuable service — helping consumers bridge short-term funding gaps. Because these loans offer high risk to lenders (greater than one in ten borrowers default on their loan), interest rates on payday loans are can be quite high. In Maine, payday lenders are required to maintain a supervised lender license with the Bureau of Consumer Credit Protection.

In Maine, the maximum fee on a payday loan of $500 or more is $25. Unfortunately, illegal loans offered by unlicensed internet-based lenders that charge interest rates in excess of 300% APR are virtually impossible for most borrowers to pay back. When a borrower gets behind on payments, these unlicensed lenders often hire unlicensed debt collectors who try to harass the borrower into paying by calling constantly, leaving threatening messages, claiming that the borrower will be arrested or trying to convince the borrower's employer to garnish the victim's wages.

If you have taken out a payday loan with an unlicensed lender, file a complaint with the Maine Bureau of Consumer Credit Protection. If the lender has access to your bank account, contact your financial institution immediately to shut the account down. See also **Aggressive/Phony Debt Collection** (pg. 14).

For a list of licensed payday lenders, contact the Bureau of Consumer Credit Protection, or view a list by visiting the bureau's website at www.Credit.Maine.gov, click on "list of license types" and select the payday lender roster.

Precious Metal Scams

Precious metal scams are a type of **investment scam** (pg. 17). In one common variation, a "metal dealer" or "merchant" offers to sell a potential victim stock or metals for 10-20% of the total price out of pocket, arranging a loan for the remaining amount. The victim is discouraged from taking physical possession of their purchase (which doesn't actually exist), or may be told that the metals will be kept safe in a "bank" or other storage location.

Although some investors use gold to diversify their portfolios and to hedge against market unrest or inflation, there is no guarantee that the value of metals like gold, silver or platinum will hold steady or rise over time. As with any commodity, investment in precious metals carries risks. Watch out for businesses guaranteeing high rates of return with no liability, never agree to purchase precious metals without verifying that the goods actually exist, and don't agree to a deal without knowing where the metal is physically located. Beware of companies that are unable or unwilling to provide proof of licensure.

Contact the Maine Office of Securities (1-877-624-8551 | www.investors.maine.gov) and the Commodity Futures Trading Commission (1-866-366-2382 | www.cftc.gov) to determine whether a business is registered to deal in precious metals commodities in the United States. Be sure to consult a financial professional when considering investing in precious metals.

"Rent-a-Creep" (Home Repair/Paving Scams)

In rent-a-creep scams, con men claim to be plumbers, builders, roofers, electricians, or other professionals. Homeowners get a knock on their door from a visitor claiming they have just finished another job and have materials left over that they need to use up — offering the consumer a deal on repairing a roof, paving a driveway, or providing other services. Sometimes the con artists offer to perform a "free" inspection, then fix any problems found for a fee. Unfortunately, the work and materials are both substandard and expensive — perhaps more so than the victim realizes until they need to get the con artist's handiwork repaired.

In Maine, door-to-door sellers of home repair services must be licensed with the Office of Professional and Occupational Regulation (OPOR), must provide a written contract, and must provide a 3-day rescission period. Before

agreeing to any kind of door-to-door repair service, ask to see the business' license. If they don't hold a license, don't do business with them! If the company appears to be unlicensed, write down the name and address of the business, names of the employees, and vehicle license plate numbers.

If you've been contacted by a door-to-door home repair business and you think the company may be unlicensed or something feels wrong, contact your local police department. If you believe that you've fallen victim to a rent-a-creep scam, file a complaint with the Maine Office of the Attorney General.

Bank Security Officer Scams

Years ago, an elderly woman in Maine was called by a "bank security officer" who told her that a teller at a local branch was stealing funds by "shorting" victims on cash withdrawals. The bank needed her help!

The woman agreed to assist, and a taxi was dispatched to bring her to the bank. When she arrived, a tall, stately man in a suit approached her in the parking lot, identifying himself as the security officer, and handed her a paper bag. The security officer instructed her to withdraw all of the money from her savings account and to place it in the bag so that he could take it back to "bank headquarters." Once there, he would count the money and, if any was missing, arrest the teller.

The woman did as she was told, brought the bag back to the parking lot and began to hand it to the "security officer." Just before giving him the money, the woman asked if the security officer could arrange for a ride back to her home. The man hesitated, and disappeared to talk with someone on the other side of the parking lot. The woman went into the bank and asked the manager about the "security officer." The puzzled manager replied, "what security officer?" The man and his accomplice had disappeared.

If an unknown person contacts you with an out of the ordinary request, get their name and title. Follow-up by calling a published telephone number for that company to verify that the request is legitimate. Never withdraw money and hand it to a person with whom you aren't familiar. If you've been contacted by or have fallen victim to a con artist posing as a security officer, get in touch with your local police department.

Tech Support Scams

Tech support scams have been around for years. A consumer receives a call from a scammer claiming to have detected a virus, malware, or other issue with the consumer's computer. After gaining the consumer's trust,

the caller may have the consumer run a series of tasks which the scammer claims will root-out the problem. Once the scammer has them convinced that there is a serious issue, they ask for sensitive personal information, remote access to the computer, or may trick the victim into installing harmful software.

If fake tech-support callers are given access to a computer they can get ahold of stored information (including Social Security numbers, bank accounts, usernames, passwords and credit card numbers). In a worst-case scenario, not only will scammers gain access to all of the information on a computer, they may also install **spyware**, malicious software that allows the scammer future access to users' information.

If you believe you've fallen victim to a tech support scam, file complaints with the Maine Office of the Attorney General and the FTC, request a file freeze (see pg. 10), and monitor your credit report. If you paid for bogus services by credit card, call your credit card provider, notify them of your situation, and ask for the charges to be reversed. Likewise, if you provided other financial information, contact your financial institution, ask for any charges to be reversed, and close your account.

Change any passwords that you gave out, in addition to those for other accounts accessed from the affected computer (family members accounts, e-mail, websites, etc.). Also update your security software, scan your computer and delete anything identified as potentially dangerous. If you do not currently have security software installed on your computer, contact your local computer retailer for recommendations. If you believe your identity has been stolen, see **Identity Theft**, pg. 7.

Timeshare Scams

In timeshare scams, a consumer is solicited to purchase an ownership interest in a timeshare. The deal ends up a nightmare when victims discover that they sent money to a crook who does not own the timeshare in question. Just because a deal looks good doesn't mean it's real — timeshare scammers often take pictures of real timeshares owned by other people and post them as their own. Another form of the

Scareware

When browsing the web one needs to be especially alert for **scareware**, automated programs designed to trick people into purchasing or downloading unnecessary and/or potentially dangerous software.

Scareware is frequently encountered through popups, e-mails and phony websites offering free security scans or claiming to have detected a virus or other malware. These alerts often look like they are being generated by the computer, when in fact they are only being displayed in the computer's browser.

scam involves offers to help sell timeshares a consumer already owns, but for a healthy fee and without any guarantee.

To protect yourself from timeshare scams, check out the company before agreeing to anything, and consider doing business only with companies that get paid after the timeshare is sold. Be sure to get all terms in writing before agreeing to anything. If you believe that you've fallen victim to a timeshare scam, file a complaint with the Maine Office of the Attorney General.

Unclaimed Property Scams

Who wouldn't love to wake up one morning and discover they found money they didn't realize they had lost? Across America, each state holds unclaimed funds in accounts with their respective treasurer's office, waiting for the rightful owners to claim the property. In Maine alone, millions of dollars of abandoned property are turned over to the state every year when the owners cannot be located.

Unclaimed property can consist of balances from inactive bank accounts, gift certificates, money orders, safety deposit boxes, uncashed insurance checks or funds from any number of other sources. In most cases you can search an abandoned property database for your name and, after filling out a few forms, claim your funds — for free!

In unclaimed property scams, con artists try to lure consumers into disclosing their name, address, date of birth and Social Security number in order to steal their identity or convince the consumers to call a number with a Caribbean area code — charging exorbitant long distance fees (see **809 Scam**, pg. 11). Some scammers offer to find money that the state is holding for a consumer for a fee, only to never provide the service.

Visit www.maine.gov/treasurer/unclaimed_property to search for undaimed property held by the State of Maine. If you believe you may have unclaimed property outside Maine, visit the National Association of Unclaimed Property Administrators (NAUPA) at www.undaimed.org.

For more information on abandoned property, contact:

Office of the State Treasurer
Abandoned Property Division
39 State House Station
Augusta, ME 04333-0039
1-888-283-2808 (Maine calls only)

Utility Billing Scams

In utility billing scams, a consumer receives a call claiming to be from Central Maine Power or another utility, and is warned that they're behind on payments. The caller claims that if the victim doesn't pay immediately — sometimes an amount several times the consumer's monthly bill — the victim's service will be terminated. Although utility scammers sometimes ask for credit card information, they're more likely to ask for prepaid cards, money orders, or wire transfers.

If you receive a call from a utility demanding immediate payment or else, don't panic. Hang up and call the utility directly, using a phone number found either on the utility's website or in your phone book, to verify whether the call is legitimate. Remember, your utility will never require you to pay a bill with a prepaid card or wire transfer.

If you believe you've fallen victim to a utility billing scam, file complaints with the Maine Office of the Attorney General and the Federal Trade Commission, as well as your local law enforcement agency.

Vacation Scams

Many prospective travelers turn to websites to find vacation rentals. Most vacation scams begin with an up-front deposit to hold the hotel, house, condo or apartment. Often, photos of actual hotels or properties are used to add legitimacy to the offer. Unfortunately, the entire vacation is ruined when the victims arrive at the airport or hotel, only to discover that no arrangements have been made. Others arrive at their destinations, only to find that the accommodations don't match the marketing, or to discover major undisclosed fees or upcharges. In some cases con artists have offered occupied homes as vacation rentals — when the victim knocks on the door they find the startled (real) owner wondering why people are at his or her door with suitcases!

Watch out for claims that you've won a free vacation, especially if you're asked to pay upfront fees. Be particularly wary if the company can't provide specifics on an offer — the more vague they are, the greater the chance that the offer is a fake. If you believe that you've fallen for a vacation scam, file a complaint with the Maine Office of the Attorney General.

Verification of Bank Account Number Scams

Some time ago, a Maine resident called to report an irregularity with his bank account. Check number 999 was showing a $200.00 withdrawal. That caught his attention. The consumer was in the 2000 number sequence with his checks — check #999 had cleared for a different dollar amount quite some time ago. When pressed, he did recall a recent call from "his banker" asking to verify his checking account number. The caller asked him to read the numbers on the bottom of the check out loud over the phone. The consumer thought the call was strange, but wanted to comply with the bank's request.

The scammer used the information provided by the consumer to raid the victim's checking account by creating and depositing a type of check called a demand draft, which doesn't require a signature from the account holder. Because the consumer notified authorities quickly, the demand draft was traced, the crook's account was frozen and the funds were reversed back to the consumer.

If you believe that you've run afoul of a verification of bank account number scam, contact the Maine Bureau of Financial Institutions.

Turning the Tables on Scammers

Received a call from a scammer? **Go on the offensive!** Try some of these comebacks...

Advance Fee Fraud

- "Just deduct the up-front payments you're asking for from the loan amount, and mail the rest to my post office box."

Aggressive/Phony Debt Collection

- "What is your Maine debt collector license number?"
  - (Hint: It must start with a DCL or a DCB, followed by a set of 3-4 numbers).
- "Tell me which sheriff's office will be serving me. I'll give them a call right after we hang up to verify. By the way, what is your name, and your company's full name and physical location?"

Credit Card APR Reduction Scam

- "I don't have a credit card."
- " I have no balance on my credit card and the APR is 0.00% for the next two years."

Imposter Scam

- "(Name), who you claim is in trouble in (country) is standing right next to me."

Investment Scams

- "This sounds like a fabulous investment opportunity. Why would you tell a complete stranger about it?" (Hang up)

IRS Scams

- "You're with the IRS? What's your physical location and direct phone number?"
- "I have a friend that works for the IRS. I want to double-check with him/her first."

Telemarketing Scams

- "Oh, my washer is overflowing. Hang on, I'll be right back!"
  - Leave the line open and find a good book to read. If they call back, don't answer. They'll eventually give up.
- "If this conversation is going to continue, I need your direct number, your company's physical address, your boss' name, and his or her direct number."

Security Officer Scam

- "If you're with my bank, why don't you know my account number?"

Glossary of Additional Terms

Adware: Software including advertisements, sometimes as pop-ups, which generate revenue for the software publisher.

Affinity Fraud: Fraud perpetrated by the leaders of a group against members of the same group (eg., service clubs, religious groups).

Boiler Room: A room full of scammers using banks of telephones to call potential victims. Calls from boiler rooms are notoriously noisy because of all the background "chatter."

Cookie: Cookie's are small packets of information put on a computer's hard drive every time that computer visits a website in order to save the user's personal information. While not inherently dangerous, cookies may be used to fraudulently gain personal information.

Dialer: Software used to connect to the internet via telephone or Integrated Services Digital Network (ISDN). Dialers are often built into a computer's operating system, and are necessary to connect to the internet for those without broadband connections. Fraudulent dialers downloaded to a computer may redirect or override a built-in dialer, connecting a victim to the internet via premium-rate phone numbers.

Hacker: A person who uses a computer to gain unauthorized access to data.

Hijacking (Computer): When a hacker takes control of a computer system. Hijacking can take many forms, ranging from resetting a browser's homepage to downloading malicious software or tampering with installed computer programs.

Key Logger: Software which records computer keystrokes in order to gather sensitive information.

Mousetrap (Java): A malicious web page which takes control of web browsers to prevent victims from leaving a website.

Ponzi Scheme: A situation in which an individual or organization pays old investors with money from new investors, in lieu of no actual profits. The infamous criminal actions of Bernie Madoff was built upon a Ponzi Scheme.

Pyramid Scheme: A business model in which victims are promised profit if they invite more victims to join and invest money.

Ransomware: A type of malware which restricts access to computer files or programs, demanding a ransom in order for the victim to regain access.

Screen logger: Software which secretly records images of a victim's computer screen in order to gather sensitive information.

Trojan Horse: An advertisement designed to draw customers by offering them money or something of value. After acceptance of the offer and signing a contract the victim is forced to spend a much larger sum than was offered to them.

Virus: Malicious software which may destroy data, steal information, or otherwise corrupt a computer system.

Worm: Malicious software which reproduces itself, spreading among computers in a network.

Maine Residents — Credit Report "File Freeze" Request Form

Use this form to request freeze your credit reports under the provisions of the Maine Fair Credit Reporting Act, 10 Maine Revised Statutes, §1310

Complete and mail by CERTIFIED MAIL to:

Equifax:	**Experian:**	**Trans Union:**
Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000

Please place a security freeze on my credit report under the provisions of 10 Maine Revised Statutes Annotated, section §1310.

SELECT ONE: ___ I am the victim of ID theft, so I am not required to pay for this freeze. Attached is a copy of a report to law enforcement.

___ I am not a victim of ID theft. Enclosed is $10 for each freeze request.

Full name (including middle name, Jr., III, etc.):

_____

Address (including zip code):

_____

_____

Social Security number:

_____

Date of birth:

_____

Former addresses for the past 5 years (if any):

_____

_____

_____

(Over)

I certify that I am the Maine consumer identified above.

Signature: _____

(Each request must contain an original signature)

Note:

1. Do not make a joint request with someone else, since each person has his or her individual credit file. For example, if spouses both want their credit files frozen, each must make a separate request.

If you have not obtained credit while living at your current address, or if you have been the victim of a severely mixed file or identity theft, then a credit reporting agency may legally request additional proof of your identity showing your current address, such as a photocopy of your driver's license, an insurance or bank statement, or a utility bill. In these cases, it will save time to include that additional information with this initial request form.

DO NOT attempt to affect someone else's credit report. Doing so is a serious crime.

EQUIFAX Experian TransUnion

Annual Credit Report Request Form

You have the right to get a free copy of your credit file disclosure, commonly called a credit report, once every 12 months, from each of the nationwide consumer credit reporting companies, Equifax, Experian and TransUnion.

For instant access to your free credit report, visit www.annualcreditreport.com.

For more information on obtaining your free credit report, visit www.annualcreditreport.com or call 877-322-8228.

Use this form if you prefer to write to request your credit report from any, or all, of the nationwide consumer credit reporting companies. The following information is required to process your request. **Omission of any information may delay your request.**

Once complete, fold (do not staple or tape), place into a #10 envelope, affix required postage and mail to:
Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281.

Please use a Black or Blue Pen and write your responses in PRINTED CAPITAL LETTERS without touching the sides of the boxes like the examples listed below:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

Social Security Number: ___ - ___ - ____

Date of Birth: ___ / ___ / ____
Month / Day / Year

Fold Here

First Name | **M.I.**

Last Name | **JR, SR, III, etc.**

Current Mailing Address:

House Number | **Street Name**

Apartment Number / Private Mailbox | **For Puerto Rico Only: Print Urbanization Name**

City | **State** | **ZipCode**

Previous Mailing Address (complete only if at current mailing address for less than two years):

House Number | **Street Name**

Fold Here

Apartment Number / Private Mailbox | **For Puerto Rico Only: Print Urbanization Name**

City | **State** | **ZipCode**

Shade Circle Like This → ●

Not Like This → ⊗ ✓

I want a credit report from (shade each that you would like to receive):

- ○ Equifax
- ○ Experian
- ○ TransUnion

○ Shade here if, for security reasons, you want your credit report to include no more than the last four digits of your Social Security Number.

If additional information is needed to process your request, the consumer credit reporting company will contact you by mail.

Your request will be processed within 15 days of receipt and then mailed to you.

31238

PUBLICATIONS

Be sure to check out other free booklets from the Bureau of Consumer Credit Protection:

- **Downeaster Common Sense Guide: Credit Reports and Credit Scores —** Learn the basics of credit, gain insight into how credit reporting and scoring work, and discover the impact your credit history has on your ability to borrow with this new publication from the Bureau of Consumer Credit Protection.

- **Downeaster Common Sense Guide: Finding, Buying and Keeping Your Maine Home** — This guide is a resource for first time homebuyers, and provides an overview of the mortgage lending process, types of mortgage lenders and loans, and other related topics.

- **Downeaster Common Sense Guide to Student Loans** — A comprehensive guide for the prospective college student on the world of educational loans. This book covers loan types, the FAFSA process, how to apply for scholarships and grants, and the rights of a student debtor in the repayment/collection process.

- **Downeaster Guide to Elder Financial Protection —** The "how-to" guide for Maine seniors who are interested in stopping unwanted telemarketing calls, pre-approved credit offers, and junk mail. This guide has sections on how to stop identity theft and how to recognize and stop elder financial exploitation.

- **Downeaster Guide: Consumer Credit 101 —** This comprehensive booklet explains the "ins and outs" of : auto-buying and financing, credit cards, mortgage loans, buying land, debt collection rights, credit reports and credit histories, plus a partial listing of Maine and federal consumer credit laws and regulations.

These guides are free to Maine residents. Out-of-state orders are $6.00 each, or at a volume discount of $4.00/copy on orders of 50 or more (shipping included).

To order, call 1-800-332-8529 (in-state) or 1-207-624-8527 (outside of Maine).

Consumer Protection Resources

Maine Bureau of Consumer Credit Protection	1-800-332-8529 TTY Maine Relay 711
Maine Bureau of Insurance	1-800-300-5000 TTY Maine Relay 711
Maine Bureau of Financial Institutions	1-800-965-5235 TTY Maine Relay 711
Maine Office of Aging and Disability Services	1-800-262-2232 TTY Maine Relay 711
Maine Office of the Attorney General (Consumer Hotline)	1-800-436-2131 TTY 1-207-626-8865
Maine Office of Professional and Occupational Regulation	1-207-624-8603 TTY Maine Relay 711
Maine Office of Securities	1-877-624-8551 TTY Maine Relay 711
Maine Public Utilities Commission (Consumer Assistance Division)	1-800-452-4699 TTY 1-800-437-1220
Maine Real Estate Commission	1-207-624-8524 TTY Maine Relay 711
Commodity Futures Trading Commission	1-866-366-2382
Consumer Financial Protection Bureau (CFPB)	1-855-411-2372 TTY 1-202-435-9742
Federal Reserve Consumer Hotline	1-888-851-1920
Federal Trade Commission Consumer Response Center	1-877-382-4357
Federal Trade Commission ID Theft Hotline **(after dialing, press "0" to reach a live operator)**	1-877-438-4338
Financial Industry Regulatory Authority (FINRA) Call Center	1-301-590-6500
Internet Crime Complaint Center (IC³)	www.ic3.gov
National Credit Union Administration (NCUA)	1-800-755-1030
U.S. Department of Veterans Affairs	1-800-729-5772
U.S. Postal Inspection Office — Portland, ME Field Office	1-877-876-2455

Maine Law Enforcement Resources

Maine Sheriff's Departments

Androscoggin	207-784-7361
Aroostook	207-532-3471
Cumberland	207-774-1444
Franklin	207-778-2680
Hancock	207-667-7575
Kennebec	207-623-3614
Knox	207-594-0429
Lincoln	207-882-7332
Oxford	207-743-9554
Penobscot	207-947-4585
Piscataquis	207-564-3304
Sagadahoc	207-443-8201
Somerset	207-474-9591
Waldo	207-338-6786
Washington	207-255-4422
York	207-324-1113

Federal Law Enforcement

FBI (Boston)	617-742-5533
FBI (Portland)	207-774-9322
U.S. Secret Service (Portland)	207-780-3493
U.S. Marshal (Portland)	207-780-3355

City Police Departments

Augusta Police Dept.	207-626-2370
Bangor Police Dept.	207-947-7382
Lewiston Police Dept.	207-513-3001
Portland Police Dept.	207-874-8575

Maine State Police

Augusta	207-624-7076 1-800-452-4664
Gray	207-756-3030 1-800-228-0857
Houlton	207-532-5400 1-800-924-2261
Orono	207-866-2122 1-800-432-7381

Maine Drug Enforcement Agency

Division One (Portland)	207-882-0370
Division Two (Houlton)	207-532-5170
Drug Tip Hotline	1-800-452-6457

NOTES

This book is not intended to be a complete discussion of all statutes applicable to consumer credit. If you require further information, consider contacting our agency or an attorney for additional help.

2nd Printing (December 2014)

Bureau of Consumer Credit Protection
35 State House Station
Augusta, ME 04333-0035
www.Credit.Maine.gov