I.D. Theft: Protecting Your Personal Information

Ed Sniffen

Senior Assistant Attorney General

Alaska Department of Law

Roots of ID Theft

- Started back in 1935 when President Franklin D. Roosevelt signed the Social Security Act.
- Everyone is given a SSN to track benefits you are entitled to upon reaching a certain age.
- Unique number – no two are alike.
- Not considered confidential. No one thought twice about giving it to anyone who asked.
- For the next 60 years, SSN's are largely in the public domain, and access to them is easy.
- Once in the public domain, difficult to "retract."
- Entrepreneurs created a business of finding, collecting, and selling SSN's for a variety of reasons. Perfectly legal.

The Game Changing Internet

- 1995 – This new phenomena called the internet comes along.
- Businesses start to use it to conduct a variety transactions – primarily advertising and selling goods and services.
- Financial institutions start using the internet to give customers the ability to access bank accounts.
- Banks start accepting applications for credit over the internet.
- This created a culture where no one had to physically “see” you before you could open an account.
- Lenders had to come up with a way to identify you before giving you credit – and they all used your SSN. With an SSN and maybe one or two other bits of personal information, anyone could open an account in your name.
- Identity Theft is born.

How ID Theft Works

- In its simplest form – ID theft happens when someone pretends to be you and opens accounts in your name. This allows the thief to get credit cards and other loans using your good credit.
- Thieves will use an address different from yours so you never get credit card statements or monthly loan invoices.
- Some thieves will actually pay the bills for a while to run up a larger credit line, then eventually take the money and run.

Your Alter Ego . . . .

- In order to convince a creditor they are who they say they are, ID thieves need your personal information. A SSN is usually the key piece of information. Other information, like your address and phone number, are easy to get once you have a SSN. With this information, an ID thief can apply for credit.

How Thieves Get Your Personal Information

- Majority of ID thieves are people you know.
- Family members, neighbors, co-workers -- all have easy access to your personal information. And you don't suspect them.
- Phishing Scams. These are fake emails and phone calls from scammers pretending to be your credit card company, utility company, law enforcement, or other entity you may have a relationship with. They ask you to verify your account information because someone has accessed your account, or for some other phony reason.
- Computer hacking. Sophisticated programs can allow hackers to get your personal information, although most ID thieves don't need to resort to that.
- Dumpster diving.
- Mail box theft.
- Simple theft of information from a business by employees, or break-in by thieves.
- Electronic data stored on old phones, computers, copy machines.
- Just about any unsecured source of personal information.

Responses to ID Theft

- From the early 2000's to today, state governments and the federal government have passed laws aimed at ID theft. Alaska's law is typical.
- In addition, financial institutions are moving away from using SSN's as the sole identifier of an individual. Identity checks are becoming more sophisticated.

Alaska's Personal Information Protection Act ("APIPA")

- Found in Alaska Statute 45.48.
- Purpose is to provide notice of security breaches involving personal information, encourage businesses and government to stop using SSN's, and provides other measures to help prevent identity theft.

Identity Theft Is . . . .

- Not Credit Card Fraud
- Prosecuted criminally under Alaska Statute 11.46.656 - .570 as “Criminal Impersonation.”
- Essentially involves someone pretending to be you and using your credit to open accounts.
- Difficult to undo.

Main Requirements of APIPA:

- Notify consumers if there is unauthorized access to personal information.
- Restriction on use, request, collection, disclosure, sale/lease/loan of SSN's.
- Allows consumers to place a security freeze on your credit report.
- Allows consumers to petition the court for a declaration of factual innocence if you are the victim of identity theft.
- Requires disposal of personal information when no longer needed.

Breach Notification

- Breach means unauthorized access of personal information
- Personal Information means last name + first name or initial AND one of the following:
  - SSN
  - Drivers license# or State I.D#
  - Account #, Credit card# or Debit Card#, unless the account can only be accessed with a PIN. If a PIN is required, then the PIN must also have been accessed
  - Passwords, PIN's, or other access codes for financial accounts.

After notice is given, no further requirement.

- The statute does not require a business or government agency to take any measures to protect personal information. Only requirement is to give notice if a breach occurs.

Exemptions

- If, after investigation and written notice to AG, you determine there is not a reasonable likelihood of harm to the consumer, then don't need to give notice. Must document this determination in writing and keep for 5 years.

- Can also delay notice if law enforcement tells you not to give notice.

If notice is required, and not given:

- Penalties: $500 for each person who is not notified, capped at $50,000
- Damages: Actual economic harm only (probably attorneys fees and costs too)

What should you do if you get a notice that your personal information has been compromised?

- Get copies of your three credit reports at www.annualcreditreport.com
- Monitor your accounts – close accounts that have been compromised (or you don't recognize)
- Consider a fraud alert on your credit reports
- Consider a security freeze
- Monitoring services may help
- Get educated – go to www.ftc.gov and review I.D. Theft information

Security Freeze

- Allows you to place a security freeze on your credit report.
- Will lock everyone out of your credit file, including yourself.
- Will not prevent you from using existing credit cards.
- Must place freeze at each of the three credit reporting bureaus: TransUnion, Equifax, Experian.
- Can only charge you $5 to place a freeze, and $2 to access your file once a freeze is in place.
- Be cautious. Very severe measure for most people.

SSN's

- Main rule – can't use, request, collect, disclose, sell, lease, loan.
- Each of these is treated slightly differently.

Use of SSN

- Can't:
  - Intentionally communicate or make an SSN available to the public.
  - Print a SSN on a card required for the person to access products or services.
  - Require a person to transmit a SSN over the internet unless it is a secure connection or is encrypted.
  - Require a SSN to access a website unless a password or PIN is also required.
  - Print a SSN on material that is mailed.

Exceptions: If you are in government and (1) authorized by law to do any of the above, or (2) necessary to perform your duties as provided by law.

Request and Collection of SSN

- Can't request or collect a SSN unless:
  - Authorized by law.
  - In government and (1) authorized by law, or (2) necessary to perform your duties as provided by law.
  - Regulated by Gramm-Leach-Bliley Act or Fair Credit Reporting Act.
  - Background check.
  - Fraud prevention.
  - Medical treatment.
  - Law enforcement or other government purpose.
  - Individual's employment.
  - Age verification.
  - For identity verification if the request/collection has no independent economic value and is incidental to a larger transaction.
  - If you are an insurer regulated by AS 21.
  - If you are a hospital corporation regulated by AS 21.87

Sale, Lease, Loan, Trade, or Rental of SSN's

- Can't do it, unless:
  - Authorized by law.
  - Regulated by Gramm-Leach-Bliley Act or Fair Credit Reporting Act.
  - Part of a credit report requested by the individual and the individual provided the SSN as part of the request.

  Knowing violation of this section is a class A misdemeanor.

Disclosure of a SSN

- Can’t disclose a SSN to a third party unless:
  - Authorized by law.
  - In government and (1) authorized by law, or (2) necessary to perform your duties as provided by law.
  - Regulated by Gramm-Leach-Bliley Act or Fair Credit Reporting Act.
  - Part of a credit report requested by the individual and the individual provided the SSN as part of the request.
  - Background check.
  - Fraud prevention.
  - Medical treatment.
  - Law enforcement or other government purpose.
  - Individual’s employment.
  - Identity verification

Penalties and Damages for Violating SSN Provisions

- Up to $3,000 maximum penalty for a “knowing violation.”
- Damages - Actual economic harm , court costs, attorneys fees.

Disposal of Records Containing Personal Information

- "Personal Information" for purposes of disposal is broader that for a security breach notification. Includes account numbers w/o names.
- Statute requires that you take "reasonable measures to protect against unauthorized disclosure" when disposing of records.
- To comply with this, you can hire a third party that is in the business of record destruction, then once you relinquish control, you are off the hook
- Must also have written policies and procedures for adequate destruction of records that are "consistent with" the statute. This means your policy should require burning, pulverizing, shredding, erasing, etc. all personal information so it cannot be read or reconstructed.

Factual Declaration of Innocence After Identity Theft

- Victims of I.D. theft can petition the Alaska Superior Court for a determination that the victim is factually innocent of a crime if:
  - The perpetrator was arrested, cited, or convicted of the crime; and
  - A criminal complaint was filed against the perpetrator; and
  - The victim's identity was mistakenly associated with a record of conviction for a crime.