EXHIBIT B

IDENTITY THEFT

What Are Identity Theft and Identity Fraud?

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

What are the Most Common Ways That Identity Theft or Fraud can happen to you?

- In public places, for example, criminals may engage in "shoulder surfing"– watching you from a nearby location as you punch in your telephone calling card number or credit card number – or listen in on your conversation if you give your credit-card number over the telephone.
- If you receive applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.
- Many people respond to "spam"– unsolicited E-mail – that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to steal large amounts of personal data.

With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes. For example:

- False applications for loans and credit cards,
- Fraudulent withdrawals from bank accounts,
- Fraudulent use of telephone calling cards or online accounts, or
- Obtaining other goods or privileges which the criminal might be denied if he were to use his real name

What Can You Do If You've Become a Victim of Identity Theft?

- Call the companies where you know the fraud occurred.
- Place a fraud alert and get your credit reports.
- Report identity theft to the FTC.
- You may choose to file a report with your local police department.

What's the Department of Justice Doing About Identity Theft and Fraud?

The Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes. In the fall of 1998, for example, Congress passed the Identity Theft and Assumption Deterrence Act. This legislation created a new offense of identity theft, which prohibits "knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." 18 U.S.C. § 1028(a)(7). This offense, in most circumstances, carries a maximum term of 15 years' imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense.

Schemes to commit identity theft or fraud may also involve violations of other statutes such as identification fraud (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344). Each of these federal offenses are felonies that carry substantial penalties –¬ in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture.

Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation, the United States Secret Service, and the United States Postal Inspection Service to prosecute identity theft and fraud cases.

FRAUD SECTION

LEADERSHIP

Daniel Kahn
Acting Chief, Fraud Section

Joseph Beemsterboer
Acting Principal Deputy Chief, Fraud Section

Christina Weidner
Chief, A&M Unit

Allan Medina
Chief, HCF Unit

Christopher Cestaro
Chief, FCPA Unit

Brian Kidd
Chief, MIMF Unit

Jerrob Duffy
Chief, Special Matters Unit

Sally Molloy
Chief, SP&T Unit

Kyle Maurer
Trial Attorney, MIMF Unit, Hiring Coordinator

CONTACT

Department of Justice Main Switchboard
(202) 514-2000

Identity Theft and Identity Fraud
Mass-Marketing Fraud
Press Releases
Speaker Requests
Career Opportunities
Report Fraud
Victim Witness Program
Contact the Fraud Section

number – or listen in on your conversation if you give your credit-card number over the telephone.

- If you receive applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.
- Many people respond to "spam"– unsolicited E-mail – that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to steal large amounts of personal data.

With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes. For example:

- False applications for loans and credit cards,
- Fraudulent withdrawals from bank accounts,
- Fraudulent use of telephone calling cards or online accounts, or
- Obtaining other goods or privileges which the criminal might be denied if he were to use his real name

What Can You Do If You've Become a Victim of Identity Theft?

- Call the companies where you know the fraud occurred.
- Place a fraud alert and get your credit reports.
- Report identity theft to the FTC.
- You may choose to file a report with your local police department.

What's the Department of Justice Doing About Identity Theft and Fraud?

The Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes. In the fall of 1998, for example, Congress passed the Identity Theft and Assumption Deterrence Act. This legislation created a new offense of identity theft, which prohibits "knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." 18 U.S.C. § 1028(a)(7). This offense, in most circumstances, carries a maximum term of 15 years' imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense.

Schemes to commit identity theft or fraud may also involve violations of other statutes such as identification fraud (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344). Each of these federal offenses are felonies that carry substantial penalties –¬ in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture.

Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation, the United States Secret Service, and the United States Postal Inspection Service to prosecute identity theft and fraud cases.

Updated February 7, 2017

Was this page helpful?
Yes No

Allan Medina
Chief, HCF Unit

Christopher Cestaro
Chief, FCPA Unit

Brian Kidd
Chief, MIMF Unit

Jerrob Duffy
Chief, Special Matters Unit

Sally Molloy
Chief, SP&T Unit

Kyle Maurer
Trial Attorney, MIMF Unit, Hiring Coordinator

CONTACT

Department of Justice Main Switchboard
(202) 514-2000