Chapter XII

Identity Theft

by Charles R. Chaiyarachta and Jonathan Fairtlough

I. Types of Victims

A grandmother living alone, an illegal immigrant, a corporation. Do they have anything in common? Yes. They can each fall victim to identity theft. And since identity theft affects many different types of victims, the charges a prosecutor files—and the information needed prior to filing—needs some consideration. Therefore, the first step in any identity theft case is to determine the number and types of victims.

There are four main groups of identity theft victims. The most common is the individual member of the public. The other three fall under organizational or corporate structures as either a corporation or public entity; a financial institution; or, finally, a merchant or service provider.

Most identity theft cases will have multiple victims that can be determined by first asking three questions: (1) Whose personal information was used to commit the crime? (2) Who provided money, goods, or services based on the stolen information? (3) Who ended up paying the money or reimbursing the provider of the goods or service? The victim that suffers the permanent loss is usually not the individual whose personal information was used—or even the merchant that provided the goods—since either or both of them will be reimbursed. The loss victim is usually a financial institution.

A. Individuals

The most common victim of identity theft is an individual who has personal information stolen that is then used to commit additional crimes. Any natural person, regardless of race, age, or immigration status, can be a victim. Additionally, a victim does not need to be alive at the time the crime is committed.[1]

1. Common methods of victimization

- Opening a credit card in the victim's name.
- Taking over a pre-existing credit card.
- Taking out a loan in the victim's name.
- Getting utility services in the victim's name.
- Buying property in the victim's name.
- Using the victim's name to set up websites, MySpace, or e-mail accounts.

2. Charges available to prosecutors

a. Penal Code section 530.5: Identity theft

The crime is committed when a piece of the victim's personal identifying information is obtained and used for an unlawful purpose without the victim's authorization.

b. Penal Code section 529.3: False personation

The crime is committed when a person pretends to be someone else in a private or official capacity and, in so doing, obtains a benefit personally or for another, or causes the victim to pay or suffer a penalty or other legal issue.

c. Penal Code section 484e-j: Access card fraud

Please note that "access card" under the statute includes a broad spectrum of potential documents and is not limited to the traditional "credit card." Also, the statutes encompass more than just the use of information. The manufacture of access cards,[2] the trading of access card information,[3] and the knowing acceptance of false access card information[4] are all criminalized in the statutes.

d. Penal Code section 470: Forgery

Many of the actions using stolen personal identifying information require a forgery to complete the crime: i.e., signing a sales slip, lease, or credit card application.

e. Penal Code sections 484 and 487: Theft

These crimes involve the taking of money, goods, or services via identity theft.

f. Penal Code section 496: Receiving stolen property

Mail theft, Dumpster diving, and other forms of information theft often involve this crime. Keep in mind that a person who accepts stolen information items is just as guilty as the person who steals personal information in printed form in order to transfer the information to another or to keep it from its true owner.

g. Penal Code section 532(a)(1): Fraudulent credit application

h. Penal Code section 472: Fraudulent documents

B. Corporate and Public Entitites

As victims, corporations and other legal entities pose unique challenges. Up until 2007, only actual corporations were considered persons under Penal Code section 7. Other business entities such as "fictitious businesses," limited partnerships, mutual companies, and public entities were not considered persons under the Penal Code.[5] But a recent addition to the Penal Code (section

530.55) specifically addressed this need to broaden the definition of "person." The definition now reads "a natural person, living or deceased, [a] firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity."

1. Common methods of victimization

Organizations become victims of identity theft in ways different than natural persons. First, many organizations have computer and telephone networks that are vulnerable to takeover and abuse. The corporation owns information such as bank accounts, telephone switches, or routing information unique to the corporation that is considered personal identifying information under the Penal Code.[6] Other common methods of victimization include:

- Purchase order fraud.
- Use of corporate calling cards, networks, or telecom services.
- Fraudulent credit applications using corporate information.
- Theft of employee information.
- Access to corporate databases by false pretenses.

2. Charges available to the prosecutor

a. Penal Code section 530.5: Identity theft

The crime is committed when a piece of the corporation's identifying information is obtained and used without the victim's authorization and used for an unlawful purpose. Most often, this involves corporate bank accounts, corporate routing numbers, or other access information owned by the corporation.

b. Penal Code section 470: Forgery

The use of a forged signature, either of a customer, applicant, or corporate officer on an application or negotiable instrument in order to obtain money, goods, or services.

c. Penal Code sections 484 and 487: Theft

These crimes involve the taking of money, goods, or services via identity theft.

d. Penal Code section 496: Receipt of stolen property

e. Penal Code section 532(a)(1): Fraudulent credit application

It is a felony to apply for credit using the information of another or by pretending to be a fictitious business.

f. Penal Code section 502(c): Computer intrusion

Access, without authorization, to a computer system run by a corporation resulting in the taking, deletion, or addition of data, or use of data to execute a scheme to defraud, deceive, extort, or wrongfully control money, property, or data.

C. Financial Institutions

Financial institutions are usually the true target of most identity thieves. The information of an individual is needed to gain access to the final goal—the money or credit provided by a financial institution. In this role, the institution is truly a victim, and one who is most likely located in another country or jurisdiction. As such, dealing with a financial institution as a victim requires an understanding of the use of the financial information available.

When an identity theft has been committed via access card fraud as specified in Penal Code section 484e,[7] a lack of consent by the victim may be proved in one of two ways. It can be shown by the cardholder testifying as to this aspect or by a representative of the issuing card company testifying that the defendant did not have permission to have the card or any of the information on it.[8] The dual nature of proving a lack of consent with Penal Code section 484e allows greater flexibility for the prosecutor that is not available with Penal Code section 530.5, the identity theft statute, which only allows a lack of consent to be proved through the individual victim.

1. Charges available to the prosecutor

a. Penal Code section 484e–j: Access card fraud

This section allows the card issuer to be the victim of the crime.

b. Penal Code section 470: Forgery

Any document sent to a company in the issuance of credit requires a signature.

c. Penal Code sections 484 and 487: Theft

d. Penal Code section 496: Receipt of stolen property

e. Penal Code section 532(a)(1): Fraudulent Credit Application

f. Penal Code section 472: Fraudulent documents

g. Penal Code section 502(c)(1): Computer intrusion

D. Merchants or Servicee Providers

The merchant or service provider is often the most overlooked of all the victims in an identity theft scam. The service station, bookstore, online retailer, or department store where the fraudulent credit is used is a victim because they are the ones who provide the merchandise to the identity thief. In many cases, if the merchant is unable to show that they properly checked

for photographic identification, they lose the value of the goods or services they provide, due to restrictions placed in credit card contracts. Another situation arises when the merchant punches the credit card numbers into a terminal instead of swiping the card through a card reader. Many credit card institutions now warn their merchants that a credit card purchase that is completed by punching the numbers into the terminal instead of swiping the magnetic strip will not be subject to reimbursement if fraud is later detected.

1. Charges available to the prosecutor

a. Penal Code section 459: Commercial burglary

b. Penal Code sections 487: Access card fraud (if merchant is card issuer)

c. Penal Code section 470: Forgery

d. Penal Code sections 487: Theft

e. Penal Code section 496: Receipt of stolen property

E. Multiple Victims and Layering

In charging identity theft, a prosecutor needs to identify all the victims. First, take a look at the different steps in the crime. A single "theft" can have three different victims: the named identity theft victim, the merchant providing the goods or services, and the institution supplying the credit.

As an example, consider a simple account takeover: The identity thief steals the mail of John Q. Public. Inside the stolen mail is Mr. Public's American Express card. Using the information from the mail, the thief calls American Express, pretending to be Mr. Public. He claims that his card was lost while on vacation, and has a new card shipped to a mailbox store. He then uses the card at Circuit City to purchase a computer.

In this scenario, there are three victims and at least eight different charges available to the prosecutor. The first victim is Mr. Public whose mail was stolen and whose personal identifying information was used without his consent. The defendant can be charged with identity theft, theft, and receipt of stolen property. The second victim is American Express as the issuer of the card. If American Express pays for the computer, the defendant can be charged with theft. Even if American Express does not suffer a loss, it is a victim of access card fraud. Finally, the third victim is the merchant, Circuit City, since it provided goods to the identity thief. The defendant can be charged with theft, forgery, and commercial burglary just for the act of buying the computer inside the store. All three victims can, and should, be listed as victims in a criminal complaint in a technique known as "layering."

Under this idea of layering, the identity thief should be charged with crimes that address each unique victim. Obviously, identity theft[9] should be charged, but other charges incorporating the actual transaction(s) should be utilized as well: theft of access card for the use of the credit card;[10] forgery for signing the victim's name at the time he purchased the goods at Circuit City;[11]

and burglary, which can be established in part by the fraudulent credit card that was on the defendant's person at the time of the transaction.[12]

To help determine the range of charges available to the prosecutor, ask the following questions:

1. **Are there lists of victim profile information in the defendant's possession?**

   A profile is a listing of a victim's personal identifying information—names, Social Security numbers, credit or bank account numbers. Many identity thieves keep lists of useful profile information in their possession, in wallets and everyday personal items like organizers or address books. If the defendant possesses the information of 10 or more persons, it is a felony; anything less is a misdemeanor. The prosecutor must show that the defendant possessed the items with the intent to defraud.[13]

2. **Does the defendant have four or more account numbers in his possession?**[14]

   Remember that an access card is not just a credit card number—it can be any code or account number used alone or in conjunction with another access card to obtain access to credit, goods, or services.

3. **Does the defendant have multiple credit or debit cards or Government identifications in other names?**

   Each card or identification in a different victim's name is a separate count and is not affected by Penal Code section 654.

4. **Did the defendant make multiple purchases or transactions?**

   Each purchase can be a separate charge of commercial burglary. Look for receipts and other items in defendant's wallet or car.

5. **Are there balance transfers to or from the victimized accounts?**

   Each transfer can be a separate count or victim. The defendant must be linked to the transfer—bank records can record the number or IP address used by the person who initiated the transfer.

6. **How did the defendant get the equipment (e.g., cell phone in victim's name, computer purchased on victim's card, internet service in victim's name)?**

   Each step can be a separate chargeable crime.

F. Vulnerable Individuals

The Penal Code provides additional punishment if the victim is considered to be especially vulnerable. If the identity theft victim is over the age of 65 or is a dependent adult as defined

by section 368(h), additional punishments apply for the misuse of the victim's information. Additional punishments also apply if the defendant is a caretaker of the victim.

Under Penal Code section 368(c), if the victim is 65 years of age or older or a dependent adult, and the defendant knew or should have known the victim's age, the punishment for an identity theft becomes two, three or four years instead of the traditional 16 months, two years, or three years. Under the caretaker fraud section,[15] if the defendant is a caretaker and commits fraud, theft, or embezzlement, the sentencing range is two, three or four years in state prison if the taking is over four hundred dollars.

G. Victim Rights and Remedies

Due to the ongoing and increasing use of personal identifying information, certain sections of the Penal Code now provide for victim remedies and rights. Section 530.6 gives a victim the right to file a police report in the jurisdiction where the victim lives, regardless of whether the illegal use of their information occurred in another judicial district. Section 530.8 gives a victim the right to obtain information about their credit accounts or to designate law enforcement as their representative in order to receive the requested information.

Civil Code section 1798.22 provides for certain rights such as the right to repair criminally damaged credit, the right to receive fraud alerts on credit histories, the right to receive notification for future credit inquiries, and the right to assert identity theft as a defense.

II. Types of Crimes

A. Fraudulent Credit Application

A fraudulent credit application is the most common form of identity theft. The thief uses the information of another person to fraudulently obtain credit, money, goods, or services. The credit application can be made in writing or electronically, such as over the phone or via the Internet.

1. Charges to consider

a. Penal Code section 532(a): Fraudulent credit application

The application itself is the crime and constitutes a business record.

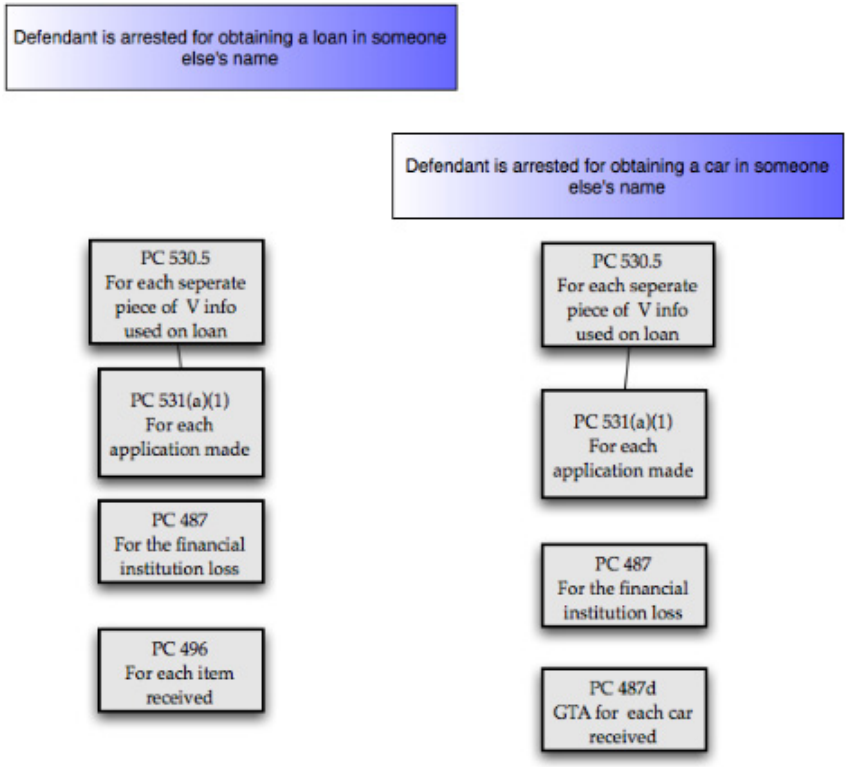
b. Penal Code sections 530.5 and 529.3: Identity theft. False personation victim

c. Penal Code section 484d and 484e: Access card fraud. Card issuer

d. Penal Code section 487: Grand theft. Financial institution as victim

e. Penal Code section 459: Commercial burglary victim. Merchants where credit is used

B. Loan Graph



C. Account Takeover (ATO)

This crime occurs when the defendant uses the information of an identity theft victim to convince a financial institution to provide access to the account of the victim. Once the thief has account access, he or she can have new cards issued, change addresses, delay or redirect statements, or lock a victim out from his or her own account by changing the personal identifying number (PIN).

1. Charges to consider

a. Penal Code sections 530.5 and 529.3: Identity theft and/or false personation

Cardholder as victim.

b. Penal Code section 484d and 484e: Access card fraud

Cardholder or card issuer as victim.

c. Penal Code section 487: Grand theft for the loss of the credit issued

Financial institution as victim.

d. Penal Code section 459: Commercial burglary merchant as victim

Commercial burglary for the business where the card was used.

D. Access Card Fraud

Access card fraud, also known as "carding," occurs when the defendant is found in possession of multiple credit cards in other people's names or is in possession of a list that contains the credit information in other people. In some cases, the defendant will also be in possession of equipment used to make or "encode" credit cards. Typical devices that are used to re-encode the magnetic strips on the back of credit cards or to make new cards altogether include computers, credit card readers, embossing machines, holograms, and silk-screens. Fake blank credit cards (that are then imprinted with the victim's information) are easily available from overseas or even on eBay. Potential charges include Penal Code sections 484e, 484i, 484j, and 502.7.

A potential problem with charging in these cases can arise if a prosecutor cannot show that the defendant used the cards that are found in his or her possession. In this situation, use section 484e(d). If the defendant possesses four or more access cards in the names of different victims, the possession with knowledge of their theft is a felony. Section 484e also covers the situation in which the defendant only possesses a list of credit card numbers, not the cards themselves. According to the definition of access card under this section, only the number is required.

Penal Code section 484e is broadly construed to include *anything* that can be used to obtain money goods or services, including just the card number itself, with or without the original piece of plastic it was printed on. In *People v. Butler*,[16] the court declared that cloned cell phones were a "means of account access," and appropriately applied section 484e. The statute also applies to access cards that are expired or cancelled.[17]

1. Penal Code section 496 versus Penal Code section 484e

Per *People v. Rowland*,[18] these two charges do not overlap for purposes of Penal Code section 654. The defendant, who kept the wallet containing the victim's credit cards for an extended period of time (somewhere between 19 hours and two weeks), was rightfully sentenced on both Penal Code sections 496 and 484e charges. The court declared "in keeping the credit cards over an extended period of time with intent to use them, he was violating a law other than that prohibiting possession of stolen property."

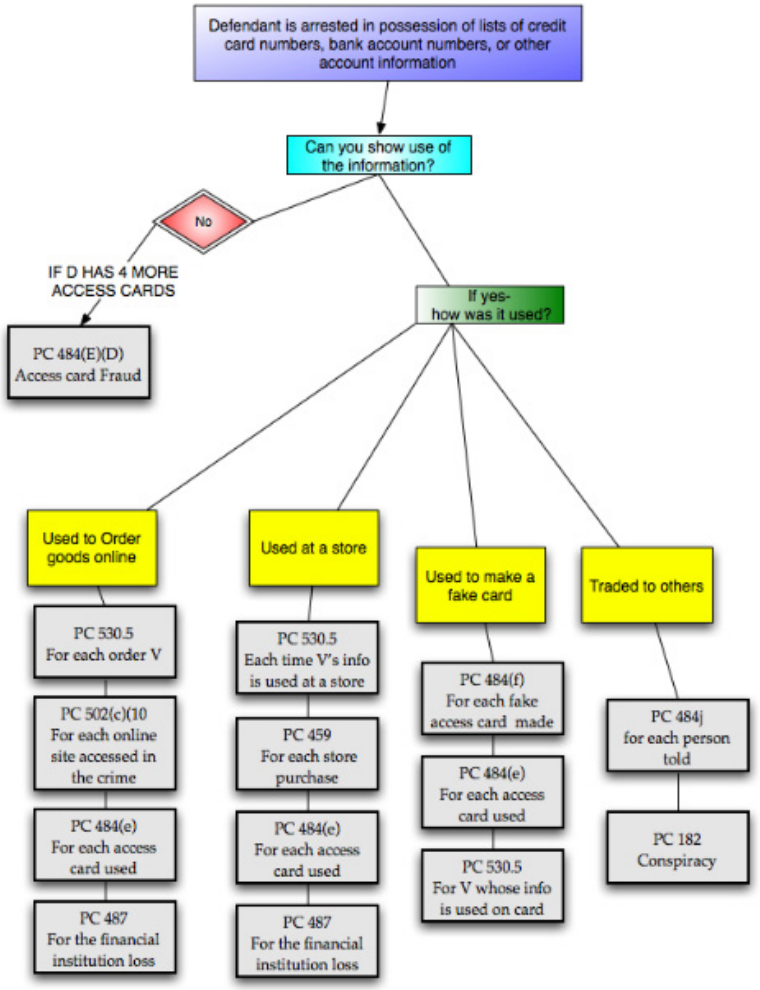
2. Penal Code section 530.5 versus Penal Code section 484e

Both Sections require the prosecution to prove that the card and personal information were used without the cardholder's consent. Penal Code section 484e, however, also allows the prosecution to prove this element by showing there was no consent by the issuer of the card instead of having to rely solely on the cardholder who may very well live out of state. This becomes significant if the individual victim or victims live out of state. In such a case, the prosecution can bring in a representative of the issuing company to prove non-consent.

3. Penal Code section 654

Possession of each access card with intent to defraud can be sentenced consecutively, if there are separate victims for each access card.[19]

E. Carding Graph



F. Loan Fraud and Merchant Bustouts

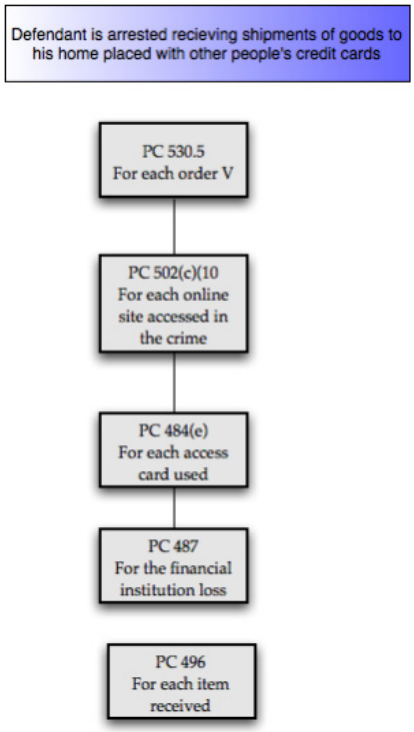
Loan fraud occurs when the purpose of the identity theft is to convince a bank or other grantor of credit to extend credit on a loan or to extend merchant credit for the payment on products. These cases take many different forms. "Padding" occurs when another person's information is used as a co-signer, or instead of the defendant's, to increase the desirability of the loan candidate.

A "bustout" is when fake sales or fake companies are used to give the appearance of financial stability in the issuance of "net terms." These cases can be very difficult to prove. Issues in these cases tend to focus on criminal intent. In most instances, the suspect will have a business documented on paper (including office location, names of employees, inventory lists, etc.) when in reality there is no such company. It is the job of the investigator and prosecutor to show that the business was set up for the purposes of committing fraud.

Practice Note: Interview any co-signers or other individuals who are claiming misuse of their names or information. Suspects will normally have a tie or relationship with co-signers that gives them access to the co-signers' information. Check to make sure that witnesses are willing to go through the challenges of a prosecution before filing.

Get company documents early. Business records can be misplaced; companies can merge. If records are going to be subpoenaed, they will need to be certified as business records. Do not assume that the company will exist later at trial to provide a witness. Look for prior bad acts when criminal intent is the issue; the suspect's prior business dealings and civil behavior can be clues to intent.

G. Dropship Graph



III. Charges

A. Identity Theft: Penal Code Section 530.5

Identity theft is committed when a piece of a victim's personal identifying information is obtained without the victim's authorization and used for an unlawful purpose. This crime does not specifically require the use of the victim's name. *Any* piece of personal identifying information (phone number, home address, etc.) can be used, alone or in conjunction with other pieces, to commit the crime.

1. Charging language: Felony: 16-two-three

Defendant did willfully and unlawfully obtain personal identifying information on victim, and used that information for an unlawful purpose and/or to obtain, and attempt to obtain, credit, goods, services, and information in the name of victim without consent.

2. Elements of the crime

- The defendant willfully obtained someone else's personal identifying information;
- the defendant willfully used that information for an unlawful purpose; and
- the defendant used the information without the consent of the person whose identifying information he or she was using.

3. Types of personal identifying information

The defendant need only use one form of personal identifying information to commit the crime.

a. Victim's personal information

This information is commonly used to take over the identity of a person and is what is commonly thought of as identity theft. Examples include a person's name, address, telephone number, mother's maiden name, date of birth, and unique biometric data such as fingerprints, facial-scan identifiers, voiceprint, retina or iris image, or other unique physical representation.

Practice Note: If the defendant has the same name as the victim but, in the use of the name, is clearly using the other's personal information or is assuming the other's identity, it is still an identity theft. In this particular situation, also consider filing a Penal Code section 529.3 charge.

Source of Evidence

- **Victim's testimony**—A person can testify to information that they have been told is part of their ancestry or background. This includes their name, date of birth, mother's maiden name, etc. Such information is an exception to the hearsay rule under the Evidence Code.

- **Government records**—Birth certificate, driver's license, etc. These records are admissible if properly authenticated as public records.

- **Physical evidence—**Fingerprints and retinal scans are obtained via scientific means. The prosecution must either have the person who obtained the evidence or a source such as a public record to authenticate the item.

b. Victim's governmental information

This type of information includes a person's health insurance identification number, taxpayer identification number, school identification number, state or federal driver's license number or identification number, Social Security number, alien registration number, government passport number, or information contained in a birth or death certificate.

Source of evidence

While it may be possible in some instances to actually get a representative of a governmental agency into court to testify about any of the public records listed above, it would be prudent of the prosecutor to also have certified copies of those records available. The items listed above qualify as public records, if the foundation can be properly established pursuant to either Evidence Code section 1271 or 1280.

In addition, some government agencies, such as the Social Security Administration, will not come to court, even under subpoena, since they are exempted from doing so under the Federal Code. This requires the prosecutor to obtain trial copies of any needed Social Security documents in advance. The Administration will also certify them, but requests must be made well ahead of time.

c. Victim's employment identifying information

This category of information includes a person's place of employment and his or her employee identification number.

Source of evidence

- **Victim's testimony—**The victim can testify as to his or her place of employment or such other personal information as his or her employee identification number or business credit card since the individual has personal knowledge of this information and would be outside the scope of the hearsay rule under Evidence Code section 1200.

- **Employer's records**—In the event that the records of the business are required, they are admissible under either of the following Evidence Code section 1271 or 1562 as long as the necessary authentication requirements have been fulfilled.

d. Victim's financial identifying information

Examples of this type of information include a person's demand deposit account number; savings account number; checking account number; PIN (personal identification number) or password; unique electronic data such as an identification number, address, or routing code; telecommunication identifying information; access device; or credit card number.

Source of records

- **Victim's testimony—**The victim can testify to this information since he or she has personal knowledge of it that would be outside the scope of the hearsay rule under Evidence Code section 1200. There is still a limit, however, as to how much information can be provided by the victim. While the individual can testify to account numbers and passwords, monthly statements from those accounts (which are usually needed to show the fraudulent transactions) must fall under a hearsay exception since those records are gathered and maintained by the bank or other institution (see below).

Financial institution's records—As stated above, when records of a business are required, they are admissible under either of the following Evidence Code sections 1271 or 1562 as long as the necessary authentication requirements have been fulfilled.

Practice Note: There are restrictions on the ability to obtain and use financial records. Prosecutors should review Penal Code section 530.8, Government Code section 7475, *People v. Blair*,[20] and Evidence Code 1563 (Payment for Business Records).

(1) No specific intent to defraud or loss needed

Identity theft is a general intent crime.[21] Penal Code section 530.5 does not require a loss in order for a crime to exist. In *People v. Hagedorn*, the defendant performed work for which he received a paycheck. The paycheck was in the name of another, and he cashed the check using the victim's license and Social Security number.[22] The defendant was convicted of commercial burglary and identity theft. He argued that there was no theft as the check was for work he performed, and that no one suffered any loss. At least two courts have disagreed, finding that:

> "[I]t is beyond question that the Legislature may, and has, defined crimes and punishments in which causation analysis plays no practical part. For example, if a defendant has possessed contraband, burglarized a premises, or battered another, criminal punishment is imposed to deter socially intolerable conduct regardless of any injury that may have been caused by the act. [Citation]"[23] In light of the indisputable evil to be remedied with respect to identity theft, the Legislature rationally appears to have concluded that willfulness, when coupled with use for an unlawful purpose, provides a sufficient mens rea for the offense, and that no injurious intent or result is required.[24][25]

(2) "Unlawful purpose" defined

The language used in Penal Code section 530.5 defines some of the actions that are considered to be uses of personal identifying information for an unlawful purpose: to obtain, or attempt to obtain, credit, goods, services, and to obtain medical information in the name of the other person without the consent of that person. But *any unlawful act* can be the purpose of the identity theft. If the information obtained is used to commit any crime, the unlawful act requirement for the identity theft statute is completed.

If the unlawful act is an attempt to obtain credit, goods, or services, the attempt is a completed act for the purposes of the statute. **There is no such thing as a Penal Code section 664/530.5 combination.** Penal Code section 530.5 lists both attempts and completed transactions as identical violations under this section.

B. Petty and Grand Theft—Penal Code Sections 484 and 487

An example of petty and grand theft is when a defendant uses a victim's information to obtain a credit card that defendant then uses at a store to obtain goods and/or services. Note that in this case, there are three potential victims: the natural person who had his or her personal identifying information used, the credit card company who issued the credit, and, finally, the retailers who provided the goods and/or services.

1. Charging language

The Defendant did unlawfully take money and/or personal property of a value exceeding four hundred dollars ($400), to wit, _____, the property of the victim.

2. Elements of the crime

Grand theft is theft committed in any of the following cases when the money, labor, or real or personal property taken is of a value exceeding four hundred dollars ($400), except as provided in subdivision (b).[26]

3. Types of grand theft common in identity theft

a. Theft by false pretenses

- A person made or caused to be made to the victim, by word or conduct, either a promise without intent to perform it or a false pretense or representation of an existing or past fact known to be false or made recklessly without information that would justify a reasonable belief in its truth; and
- the person made the pretense, representation, or promise with the specific intent to defraud; and
- it was believed and relied upon by the victim and material in inducing him or her to part with money; and
- the victim actually gave money or property.

b. Theft by trick or device

- A person obtained the personal property of the victim; and
- that person obtained the property by making a false promise, which he or she had no intention of performing, or by other fraud; and
- the victim did not intend to transfer ownership; and
- the person had the specific intent to permanently deprive the victim of said property.

4. Necessary documents and witnesses

- The person who provided the property or money to the defendant.
- Someone to testify as to the value of the goods/services/money provided. See Evidence Code sections 813 and 823 regarding the valuation of property.

C. Stolen Mail—Penal Code Sections 496 and 530.5(c)(3) & (e)

The defendant, in addition to committing identity theft or another related crime, has in his or her possession numerous credit applications, credit cards, monthly credit card statements, utility bills, etc. that were stolen from the victims' respective mailboxes. The stealing of mail from neighborhood mailboxes has become so common among ID thieves that they refer to it as "mailing" or "jogging."

1. Charging Language

Defendant did unlawfully buy, receive, conceal, sell, withhold, and aid in concealing, selling, and withholding property, to wit, U.S. MAIL, which had been stolen and obtained by extortion, knowing that said property had been stolen and obtained by extortion.

Practice Note: In the event that the mail belongs to a victim who lives outside the prosecutor's jurisdiction, using Penal Code section 497 should be considered. Specifically allege theft or receipt of stolen property in another county.

Defendant did unlawfully buy, receive, conceal, sell, withhold, and aid in concealing, selling, and withholding property, to wit, U.S. MAIL, which had been stolen and obtained by extortion, knowing that said property had been stolen and obtained by extortion.

It is further alleged that on and about _____, property was brought into this County and that said Defendant did unlawfully bring said property unlawfully taken and received in Name of other state or country to the County _____, State of California within the meaning of Penal Code section 497.

2. Elements of the Crime[27]

To prove that the defendant is guilty of this crime, the People must prove that:

- The defendant bought, received, sold, aided in selling, concealed, or withheld from its owner, or aided in concealing or withholding from its owner, property that had been stolen or obtained by extortion; and
- when the defendant bought, received, sold, aided in selling, concealed, or withheld or aided in concealing or withholding the property, he or she knew that the property had been stolen or obtained by extortion.

3. Filing Consideration

Usually, when an ID thief is involved in mailing, he or she will possess mail from numerous victims. As the case below outlines, unless the prosecutor can show that mail from each victim was received on various occasions, Penal Code section 654 will apply, and the defendant can only be convicted and sentenced on one count of Penal Code section 496, regardless of how many victims are involved. A defendant who receives more than one item of stolen property on a single occasion commits one offense of receiving stolen property.[28]

As of 2007, additional Penal Code sections may apply to a defendant who is involved in "mailing" or "jogging." Penal Code section 530.5 now includes section (c)(3) that makes it a crime to possess the personal identifying information of 10 or more individuals. Chances are, if a defendant is stealing mail, the goal is to obtain credit card numbers, checking account numbers, or similar information, which are all listed in Penal Code section 530.55.

In addition, the theft of mail itself (regardless of what information contained therein) has been added to the Penal Code by way of section 530.5(e).

D. False Financial Statement—Penal Code Section 532a

Example: The defendant uses the victim's name and Social Security number to obtain a loan on a new car. Based on this fraudulent information, the car dealer approves the loan when it otherwise would not have.

Practice Note: It is not enough that the defendant used someone else's personal information. The prosecution must prove that the fraudulent information was relied upon to deny or grant credit.[29]

1. Charging language

a. Penal Code section 532a(1)

The defendant did unlawfully make, and cause to be made, a false financial statement in violation of this section by using a fictitious name, social security number, business name, and business address, and by representing himself or herself to be another person and/or another business.

b. Penal Code section 532a(2)

The defendant did unlawfully benefit from a false financial statement in violation of this section by using a fictitious name, Social Security number, business name, and business address, and by representing himself or herself to be another person and/or another business.

c. Penal Code section 532a(3)

The defendant did unlawfully reaffirm a false financial statement in violation of this section by using a fictitious name, Social Security number, business name, and business address, and by representing himself or herself to be another person and/or another business.

2. Elements of the crime

- The defendant made or caused to be made a false written statement about his or her financial condition or means or ability to pay; and
- the defendant knew that the statement was false; and
- when the defendant made the statement or caused the statement to be made, he or she intended that the statement be relied on; and

- the defendant made the statement or caused the statement to be made to obtain the delivery of personal property; payment of cash; making of a loan; extension of credit; execution of a contract of guaranty or suretyship; discount of an account receivable; or the making, acceptance, discount, sale, or endorsement of a bill of exchange or promissory note for his or her benefit or the benefit of the other person or corporation.

3. Necessary witnesses and documents

- The credit application.
- The loan officer who assisted the defendant. (Can he or she identify the defendant? Was there a delay in approving the loan? If so, is another witness needed to testify that the loan was approved, and it was approved, based in part, on the false information provided by the defendant?)
- The victim, whose information was used on the credit application, to testify that there was no permission to use the personal information.

Practice Notes: A prosecutor does not need to prove that the defendant made the application personally; merely that he or she caused it to be made. The application does not have to be in writing. The victim must rely on the application in the grant of credit. There is no duty on the part of the victim, however, to make any form of investigation into the veracity of the statements in the application. If the victim company does make its own investigation, and it should have discovered the fraud, it can be bound by its failure.

E. Access Card Fraud

Access card fraud encompasses any form of theft via an access card, or any part of it. The different Penal Code sections cover different types of crimes using access cards, but the definitions are the same.

1. Definitions

a. Cardholder

A cardholder is any person to whom an access card is issued or any person who has agreed with the card issuer to pay.

When an account has multiple cards issued, either the person whose name is on the card or the person responsible for the account can testify as the cardholder.

b. Access card

An access card can be a card, plate, code, account number or other means of account access that can be used, alone or in conjunction with another access card, to obtain money, goods, services, or any other thing of value or that can be used to initiate a transfer of funds other than a transfer originated solely by a paper instrument.

This means that a check cannot be an access card. A balance transfer or a wire or debit payment qualifies as an access card. An access card does not require that there be an actual physical card.

Examples of an access card include a credit card number written in a notebook; an AOL.com username and password used to order items; an online bill-pay transaction; an airline-mileage account number and PIN; a company purchase order number used to bill; or a cell phone number used to order phone services.

An expired access card is an access card that shows on its face that it has lapsed.

An access card is incomplete if anything other than the signature of the cardholder is missing from a card.

A revoked access card is an access card that is no longer authorized for use by the issuer. Authorization can be suspended or terminated. Written notice must be provided to the cardholder.

A counterfeit access card is any access card that is counterfeit, fictitious, altered, or forged, or any false representation or depiction of an access card or part of an access card.

c. Card issuer

A card issuer is any person who issues an access card or is the agent of the issuer of the card.

d. Retailer

Every person who is authorized by an issuer to furnish money, goods, services, or anything else of value upon presentation of an access card by a cardholder is a retailer.

e. Traffic

Traffic is the act of transferring or otherwise disposing of property to another or obtaining control of property with intent to transfer or dispose of it to another.

f. Card making equipment

Card making equipment is any equipment, machine, plate, mechanism, impression, or other device designed, used, or intended to be used to produce an access card.

Practice Note: If there are facts that show a suspect in possession of equipment that can be used to encode information on a card, a series of misdemeanor violations for encoder use or encode possession is available under Penal Code section 502.7. Remember that a felony conspiracy to commit a misdemeanor charge can also be used.

2. Penal Code sections 484e and 484g

The difference between the four subsections of Penal Code section 484e:

484e(a)—When the defendant sells, transfers, or conveys an access card with the intent to defraud, he or she is guilty of grand theft.

484e(b)—When the defendant possesses more than four access cards within a 12-month period with knowledge that the cards have been stolen or retained in violation of the theft statute, he or she is guilty of grand theft.

484e(c)—When the defendant, with the intent to defraud, possesses an access card with the intent to use, sell, or transfer it, he or she is guilty of petty theft.

484e(d)—When the defendant possesses an access card and intends to use it fraudulently, he or she is guilty of grand theft.

Penal Code section 484g—The fraudulent use of an access card or account information occurs when a person with the intent to defraud, either (a) uses an altered, forged, or stolen access card or (b) falsely represents himself or herself as the card holder and obtains money, goods, services or any other thing of value.

3. Penal Code sections 484f and 484i

484f(a)—When the defendant, with the intent to defraud, either designs, alters, embosses, or makes a counterfeit access card, or utters or attempts to utter a counterfeit access card number, he or she is guilty of grand theft.

484f(b)—When the defendant, with intent to defraud, signs either a fictitious name or the name of another to a sales slip or transaction on an access card, he or she is guilty of forgery.

484i(a)—When the defendant possesses an incomplete access card with the intent to complete it, he or she is guilty of a misdemeanor.

484i(c)—When the defendant possesses any card-making equipment with the intent of making complete access cards, he or she is guilty of a felony.

4. Evidence needed to prove access card fraud

- The business records of the card issuer or a statement from the purported issuer showing that they did not issue the card. (The prosecution will need a representative of the victim issuer to testify.)

- The witnesses who observed the defendant utter, or attempt to utter the access card number, or sign the sales slip that relates to the access card.

- If the 484f or 484i series is used, the prosecution will need a technical witness who can testify that the cards were manufactured or that the equipment recovered is for the purpose of manufacturing access cards. (Contact the issuer—each card will have its own security features and specific methods for identifying fake plastic. The issuer will usually have a witness available to make that determination and testify to it. Do not wait until the week prior to trial to get the cards examined.)

F. Enhancements

Depending on the amount of loss, certain enhancements can be charged under the Penal Code that will either add a mandatory jail sentence or add time to a state prison sentence.

1. Pattern of felony conduct with a loss over $100,000—Penal Code section 186.11

If the defendant is convicted of two or more felonies that involve a pattern of fraudulent conduct, he or she shall be punished by an additional term of two, three, or five years. If the loss is over $100,000 but less than $500,000, Penal Code section 12022.6 shall apply.

2. Taking of property over $50,000—Penal Code section 12022.6

- If the defendant takes property over $50,000, the court shall impose an additional one-year term.
- If the defendant takes property over $150,000, the court shall impose an additional two-year term.
- If the defendant takes property over $1,000,000, the court shall impose an additional three-year term.
- If the defendant takes property over $2,500,000, the court shall impose an additional four-year term.

G. Mandatory Jail Time

1. Economic Crime Act—Penal Code section 1203.044

If the defendant has been previously convicted an offense with a Penal Code section 12022.6 enhancement, probation shall not be granted if the new crime involves a taking over $50,000

Probation under this section shall not be granted to a person who is convicted of taking more than $100,000 in a single transaction or occurrence, except in an unusual circumstance.

2. Limitation on granting probation—Penal Code section 1203.045

Probation under this section shall not be granted to a person who is convicted of a crime or theft of an amount exceeding $100,000. (Note that this section does not directly specify that the theft had to occur in a single transaction).

IV. Filing Issues

A. Filing the Identity Theft Case

The first question to address in the filing review of an identity theft case is, "Who are my victims?" In most cases, there will be many different victims of many different types. The question list below will help in determining the victims and necessary witnesses of a case.

1. Victim checklist

- Who are the victims? Who suffered the loss? The individual who had his or her information used, the bank who took a loss for the fraudulent credit card purchase, the retailer who sold goods based on the fraudulent transaction?
- Where do the victims reside?
- Will the victims testify? For financial institutions who are based out of state, do they have a local representative?
- If an individual victim will not testify, can a financial institution representative testify instead of the victim?
- Are the necessary documents available?

2. Evidence checklist

a. Account takeover

Copies of the "print screens." These are exact copies of what the credit card customer service representative looks at when checking on or updating the status of a person's account over the phone. It will show the date and time the account was taken over and possibly the phone number used to call into the credit card company. It is common for a defendant to use the same phone number(s) to open up accounts. A representative from the credit card company will have to testify as to the authenticity of the business records.

b. Fraudulent credit card account

Some credit card companies, such as American Express, keep copies of the actual application for credit if it was done by mail. If it was completed using the internet, some companies will keep an electronic copy of the application and possibly have an IP log as well.

c. Recordings of the transaction

Some retailers (Target, for example) are equipped with computer recording devices that videotape each transaction and store it by receipt number and/or the checking or credit card number used.

3. Bail motion—Penal Code section 1275.1

The prosecution should consider filing a bail motion if it can be shown that the defendant profited from the crimes alleged. This motion can be filed by either the arresting or the prosecuting agency. Basically, it requires the defendant to show the source of bail. The magistrate must be satisfied that the bail proceeds were not the monetary profits from the defendant's crime spree. Section (a) states, "Bail … shall not be accepted unless a judge or magistrate finds that no portion of the consideration, pledge, security, deposit, or indemnifications paid, given, made, or promised for its execution was feloniously obtained."

B. The Issue of Identity: Determining Who Actually Called Customer Service to Take Over the Account

From the credit card companies, request automatic number identification (ANI) and caller ID records of telephone numbers used to call into accounts. ANI numbers can be referenced to regarding date and time of call, and to cross-reference the customer service call.

Regarding victims: If the cardholder lives in another state, use Penal Code section 484e rather than section 530.5 as the charge. The credit card issuer can then be used as the victim.

V. Conclusion

The crime of identity theft has become increasingly prevalent within the last 12 years. With the now common use of computers and the internet, the access to personal identifying information has grown at the same rate.

Prosecutors who are assigned to these cases should be prepared to obtain the numerous documents that are required for a successful resolution. It may appear daunting, but it is not insurmountable. With the proper planning, a judge or jury can be shown exactly how the defendant committed these crimes through witnesses and business records. Finally, different Penal Code sections can be used to address specific victims of the same crime scheme.

ENDNOTES

1. See *Lee v. Superior Court* (2000) 22 Cal.4th 41[false personation applies to impersonation of deceased]; Penal Code § 530.55.
2. Penal Code § 484i.
3. Penal Code §§ 484d and 484e.
4. Penal Code § 484f.
5. *People v. Schomig* (1925) 74 Cal.App. 109, 113 (co-partnership was not a "person" pursuant to Penal Code § 7); but see 34 Ops.Atty.Gen. 98 (1959) ["person" as used by Penal Code § 7 includes incorporated correspondence schools as well as other business associations].
6. Penal Code § 530.55(b).
7. See Penal Code § 484d(2) for the definition of "access card," which is much broader than simply the traditional credit card.
8. See Penal Code § 484e.
9. Penal Code § 530.5.
10. Penal Code § 484e.
11. Penal Code § 470(d).

12. Penal Code § 459.
13. See Penal Code § 503.5(c).
14. See Penal Code § 484e(d).
15. Penal Code § 368(d).
16. *People v. Butler* (1996) 43 Cal.App.4th 1224.
17. *People v. Molina* (2004) 120 Cal.App.4th 507.
18. *People v. Rowland* (1971) 21 Cal.App.3d 371.
19. *People v. Butler, supra.*
20. *People v. Blair* (1979) 25 Cal.3d 640.
21. *People v. Hagedorn* (2005) 127 Cal. App.4th 734.
22. *Id*.
23. *People v. Jackson* (2000) 77 Cal.App.4th 574, 578.
24. *See People v. Rathert* (2000) 24 Cal.4th 200, 205–206.
25. *People v. Hagedorn, supra,* 127 Cal. App.4th at 744.
26. Penal Code § 487(a).
27. Penal Code § 496(a).
28. See *People v. Dominguez* (1995) 38 Cal.App.4th 410 and *People v. Lyons* (1958) 50 Cal.2d 245.
29. *People v. Vincent* (1993) 19 Cal.App.4th 696.

Charles (Chuck) Chaiyaracta and Jonathan Fairtlough are both deputy district attorneys in Los Angeles County.

Appendix A

Filing an Identity Theft—A Prosecutor's Checklist

1. Who was victimized?

a. Member of the public
b. Corporation or public entity
c. Financial institution
d. Merchant, retailer, or credit processor

2. What kind of personal identifying information (PII) was used?

a. Name
b. Address
c. Date of birth, Social Security number, driver's license, or identification card
d. Passport or alien registration card
e. Unique electronic data
f. Information from an access card, a credit card, or store account
g. Checking account information
h. Biometric data

3. What was the PII used for?

a. Credit card account takeover (ATO)
b. New fraudulent credit account
c. Unsecured loan (i.e., car loan)
d. Secured loan (i.e., purchase real property)
e. Medical services
f. Gain access to a system
g. Obtain utility services
h. Revenge

4. Who has jurisdiction?

a. Where was the PII obtained?
b. Where was the PII used?
c. Was the PII used in more than one location?
d. Where was the effect of the crime felt?
e. Is there other activity in a contiguous count?
f. Where is the evidence located?

5. What was the loss?

a. How is the loss calculated?
b. How is it related to the use of PII?
c. Who suffered the loss?
d. Is there more than one victim?

This page intentionally left blank.