Using Enhanced Jurisdictional Laws to Prosecute Multi-County Identity Thefts

by Howard A. Wise and Joe Williams, Jr.

California prosecutors have been entrusted with a powerful, unique but little-used tool to fight identity theft, Penal Code section 786(b). As of January 1, 2010, prosecutors are allowed to charge in one county, all identity thefts and "all associated offenses" that are "the same scheme or substantially similar activity."[1] The identity thefts can occur in multiple counties, the victims can reside in multiple counties, and the victims' information can be used in multiple counties—and the case may still be prosecuted in **any** county where one (or more) of these things occurred. To guard against prosecutorial overreaching, after the filing of a complaint in the prosecuting county, the court must hold a hearing to determine whether the matter should proceed.

The Legislature increased the territorial jurisdiction for identity thefts in 2009 because law enforcement benefits by (1) not having to conduct duplicitous investigations in numerous counties, and (2) has the ability to try all cases at once rather than having several similar trials in multiple counties. The defendant is benefited by the opportunity to resolve all outstanding criminal liability in one trial.[2] Additionally, showing involvement in similar schemes helps prove the criminal intent and prove lack of mistake on behalf of the perpetrator and co-conspirators; it also helps consolidate losses to improve the ability to prove a taking of $100,000 or more. This makes a defendant eligible for state prison and allows for enhanced forfeiture procedures to make victims whole.

This article focuses on using section 786(b) to prosecute identity thieves who place "skimmers" on ATMs and gas pumps while moving from jurisdiction to jurisdiction. The strategies and procedures are also applicable to many other multi-jurisdictional identity thefts.

APPLYING PENAL CODE SECTION 786(b) TO THE TYPICAL SKIMMER CASE

The Crime and Its Detection

"Skimming"[3] is done in three steps. First, organized groups[4] and individual criminals (made savvy by the Internet) place "skimmers" that copy electronic Personal Identifying Information (PII) from magnetic strips on debit and credit cards used at ATMs and gas pumps. The skimmer can also be placed on the door access mechanism that allows access to vestibules that house ATMs at banks. Typically, a disguised camera[5] is also strategically placed near the keypad to capture the victim entering his or her PIN number. Skimmers may use Bluetooth capability to wirelessly transmit the electronic PII to a nearby remote location, but it is in the criminal's interest to check, retrieve, and re-use the equipment. Groups will often travel from Los Angeles to San Francisco, hitting targets along the way.

Second, the skimmed electronic PII is re-encoded onto the magnetic strip of new cards that are often generic cards accompanied by handwritten numbers and PINs, or they may look like legitimate cards.

Third, the re-encoded cards are used in ATMs and "point of contact" stores such as Wal-Mart to buy goods or gift cards, or to withdraw money. Step three is the obvious way that the skimmer can make a profit, but the victim's PII can also be sold on the Internet or traded for drugs or bartered. The skimmed information may then be used anywhere in the nation.[6]

continued on page 28

MULTI-COUNTY IDENTITY THEFTS from page 27

Skimming suspects are often caught when one member of the group arouses the suspicions of a passerby or, more frequently, is detected by security officers from banks or credit card companies that remotely monitor cameras and then alert law enforcement. Alerted police wait for the crook to return to check on or remove the skimmer or camera. The crook is arrested and his car is searched. Other members of the group who are engaged in counter surveillance[7] profess ignorance or escape undetected.

Building the Bigger Case

Organized groups can obtain the equipment they need from foreign countries or buy it on the Internet. International contacts also help launder funds and procure bail bonds. Skimming gangs often travel from county to county within states. They also travel and send money interstate and internationally.[8] They put skimmers on ATMs at banks and in gas station pumps. Different members of the group install, uninstall, and "cash out the cards." They might wear hats or sunglasses and change or switch clothes to avoid detection. Clothes and other instrumentalities of the crime used during skimmer installation are sometimes left with a confederate at the time of equipment removal. Therefore, even if police arrest the person who comes to un-install the skimmer, other confederates might not be detected and can leave with important evidence. Additionally, when arrested, suspects often provide false names and false addresses, which makes executing successful search warrants challenging.

To build a bigger case, quick initial action must be taken.

High Bail and Source of Bail

High bail should be obtained based on the multiple identity thefts and lack of ties to the community.[9] False names are often used. Fingerprints and immigration status should be checked. If allowed by law, cards with a magnetic strip on the back should be run through a card reader to determine if another person's PII has been embedded on the card.

If appropriate, a peace officer and/or prosecutor should then file a declaration setting forth the reasons why there is probable cause to believe that the source of the bail will have been feloniously obtained.[10] If this declaration sets forth the facts of the offenses occurring in several jurisdictions, it can also be used for the motion to establish jurisdiction pursuant to Penal Code section 786. A magistrate then determines whether probable cause has been established to believe proffered bail will be feloniously obtained. If probable cause is established, the burden shifts to the defendant to show by a preponderance of the evidence, at a hearing, that the bail funds were not feloniously obtained. This hearing can provide significant intelligence about the defendant's associates.

Contact with Bank Security

Prosecutors and investigators should identify the decision makers in the security offices of affected institutions because those are the people who have the ability to commit to providing all necessary witnesses. Typically, they will be the ones supervising bank security officers housed at remote locations. Security officers may know of skimmings that are never reported to law enforcement. For example, if a successful and undetected skimming occurs in City A, then bank personnel might not know about it until days or weeks later. It is only discovered when re-encoded cards are used to "cash out" in Cities B, C, and D, and victims complain of getting billed for unauthorized transactions. It then takes a period of time for bank security to establish that PII was obtained from the same point of compromise in City A, and the time of that compromise. Video is then reviewed to look for the suspects.

Frequently, none of this activity will be reported to law enforcement; banks will merely notify victims of the breach and make them whole. In a best-case scenario, bank security from the affected bank in City A is working in an organized way with security personnel from other banks, credit card companies, and large retailers, but this is rare.

Bank security may have proprietary "red flags" in their system for detecting fraud that they do not want discovered to the defense or publicly disseminated. At times, however, the use of a particular item or artifice tips the bank to an ongoing skim. Recovery of that item by law enforcement from the target or confederates becomes significant. For example, the use of a particular set of PII embedded on a card or even a specific type of card might be significant if seized from the defendant(s).

Banks may have records and video of other times and places that suspect PII have been used and when the target has used other cards, legitimately and illegitimately. Looking at those videos and records can identify other crimes committed by the defendant and confederates. Moreover, often co-conspirators can be identified in a video that takes place between the hour before install and the time of removal of skimmers and cameras for evidence of confederates checking on the equipment, jamming up other ATMs to force other customers to use the compromised machines, or repeatedly entering cards during a "cash out."

Preservation of Records

It is important that the store or bank preserve the records and videos in a manner that will allow them to be used in court. In particular, the records of transactions, and the video and any metadata in the video, must be able to be authenticated and meet hearsay objections. Care should be taken to review the intricacies of laying these foundations in compliance with the Evidence Code. However, in general terms, the financial institution needs to be able to provide an affidavit and potentially a live witness[11] that describes:

- the specific identity of the records;
- that the records provided are what they say they are;
- the reasons why they believe the computer and/or video system that captured the transaction records, video, and video metadata (date, time, and location) appeared to be working; and
- compliance with the applicable Evidence Codes sections (see §§ 1271, 1560, and 1561 relating to business-record exception to the hearsay rule).

Large institutions such as banks (and their attorneys) might be resistant to signing an affidavit that is not their standard affidavit. The prudent prosecutor will either require a sufficient affidavit or the personal appearances of a legally competent witness or witnesses in court. In determining the witnesses needed, anticipate that the witness from an entity needed for video might be different than the witness needed for transaction records.

Follow up on Seized Phones, GPS Devices, Cameras, and Skimmers

Phones and GPS—It is common for organized groups of identity thieves to communicate using a "burner phone," a cheap phone that is used only for the specific mission and then discarded (a.k.a., "burn" phone). That specific "mission," however, often involves several skimmings in different jurisdictions. Additionally, even identity thieves have loved ones, so they often carry a "clean phone" to communicate with them, often around the time and in the place where they are committing crimes. Both "burner" phones and "clean" phones contain important

continued on page 30

MULTI-COUNTY IDENTITY THEFTS from page 29

information. Forensic examination might lead to obvious evidence, including communication among the thieves and photos that show that they are engaged in a joint venture.

Cell phones and smart phones also contain valuable information that is not immediately apparent, called "metadata," that can help identify the location of other skimmings. Depending on how users have configured their smartphones, images often include metadata regarding the location (in longitude and latitude), dates photos were taken, and other information.

Search warrants should be served on the cell phone providers of any phone that can be connected to the crime, especially phones seized at the scene of a skimming. Cellphone providers can provide cell tower site or "tower dump" information that provides the latitude and longitude of the cell towers the phone used to facilitate calls and texts. Thus, while this will not pinpoint a cell phone location at a given ATM, by "triangulating" the cell tower locations in a general location, technicians can usually come within a couple miles. The investigator or analyst must convert the longitude and latitude to physical addresses by using programs such as Google Earth, and proprietary information held by the cell phone providers regarding the location of their towers. While the tower dump information is easily understood at a superficial level, a true understanding of the technology and legal considerations necessary for presenting it in court requires specialized training.[12]

If a stand-alone or embedded GPS device is seized from a target's car, it might contain the addresses of targeted banks, gas stations, or retail stores. This information can be synced to video of the crimes kept by banks to corroborate the target's presence in the video at multiple crime locations. This is important because bank video, standing alone, is often not enough to prove guilt beyond a reasonable doubt. When the target is tied to multiple theft locations by both video and phone records, it reduces the chance of misidentification and establishes the target's intent and knowledge.

Skimmers and GPS—Police will often seize skimmers and disguised cameras. These require specialized forensic examination and handling. With proper care and procedures, information can be retrieved from storage memory in these devices. The United States Secret Service is a leader in the area of skimmer forensics, but cameras can often be examined by less specialized forensic experts. Additionally, DNA can be obtained from the interior of cameras and skimmers because setting them up is a delicate operation that is often done without gloves.

TASK FORCES, STATE AND FEDERAL PROSECUTORS

Seeking and sharing information from established task forces is an invaluable tool when investigating skimmer and other multi-jurisdictional cases. Most regional high-tech task forces[13] have an identity theft component. When the targets are from Burbank, Glendale, or other San Fernando Valley areas, task forces such as the Eurasian Organized Crime Task Force,[14] the Los Angeles Fraud Task Force,[15] the Southern Nevada European Organized Crime Task Force, a.k.a., the Transnational Organized Crime Task Force (based out of Las Vegas),[16] and the Southern California High Tech Task Force Identity Theft team[17] are excellent resources for identification of photographs, intelligence, and strategies.

Contacting a task force is also an excellent way to involve agencies such as the Secret Service, FBI, and the United States Customs and Border Protection (CBP) component of the Department of Homeland Security,[18] and obtain Financial Crimes Enforcement Network (FinCEN) and Social Security Administration records. The Secret Service is particularly, and often uniquely, well-suited to handle forensics on

seized skimmers and cameras. If a Secret Service agent is willing to work on your case and coordinate with other Secret Service offices that have information or evidence, it will greatly improve your investigation. A federal "law enforcement officer" may be a Proposition 115 hearsay witness in a preliminary hearing.[19]

Federal prosecution by the United States Attorney's Office (USAO) is often the most attractive option for prosecution because significantly longer sentences can be meted out.[20] For example, federal prosecutors receive significant sentencing enhancements based on the number of victims.[21] On the other hand, federal prosecutors can be selective about the cases they choose to prosecute, and turning the matter over to the USAO means the state prosecutor loses control over how, when, and possibly if, the case is prosecuted. An attractive hybrid option, if geographically feasible, might be to have a deputy district attorney cross-designated as a special assistant United States attorney.

The California Office of the Attorney General has an e-Crime Unit that is also an excellent resource because they are experienced in handling multi-jurisdictional identity theft cases. Experienced prosecutors are available to help anywhere in California. Moreover, the DAGs assigned to the eCrime unit will assist in the manner requested by the local prosecutor, including consultation, second-chairing, or handling the cases alone. The DAGs have a distinct advantage in handling these cases that a single local prosecutor does not enjoy: DAGs have the ability to handle the prosecution in one jurisdiction or several jurisdictions.

Charging the Multi-jurisdictional Identity Theft Case

Choosing your Charges and Victims

There is little to no published case law specifically interpreting Penal Code section 786(b) in its current form. This gives the plain wording of the statute added import. One such example is the phrase "[j]urisdiction also extends to all associated offenses connected together in their commission to the underlying identity theft."[22]

In multi-jurisdictional identity theft prosecutions, it is often best to include charges that do not require individual skimming victims to travel long distances. Because individual victims likely have been made whole by their financial institution, they have little incentive to travel long distances. Yet, the traditional identity theft charge has an element that requires proof that the victim's PII be obtained "without the consent of that person."[23] Prosecutors feel most comfortable proving this through the cardholder's direct testimony that he or she did not give permission. If there is a known "person" who is a victim, this element can also be proved circumstantially by the manner in which the PII was stolen in a mass skimming at an ATM or gas station. To this end, there is no substitute for the prosecutor going to the police station to personally view all of the tools of the trade seized during the arrest.

State Prison Eligible Charges and Seizing Assets for Restitution

During prison Realignment, identity thefts (and most theft crimes) were classified as crimes that do not qualify for state prison.[24] The most notable exception that may allow for a state prison sentence is when a crime that has the element of fraud leads to a taking of more than $100,000.[25] The advantage to charging offenses provable with banks as victims, rather than individual civilian victims, is that it can require hundreds of individuals to prove a $100,000 taking. Financial institutions, however, can easily sustain losses exceeding $100,000 as they typically reimburse their victims for losses. As with assessing any victim's loss claim, the assigned prosecutor must carefully review claims of loss from banks to make sure that all claims are provable at a preliminary hearing and trial.[26]

continued on page 32

MULTI-COUNTY IDENTITY THEFTS from page 31

Crimes provable with just financial institution and law enforcement witnesses that do not require proof of a civilian victim's lack of consent, and include an intent to defraud that is likely to satisfy Penal Code section 186.11, include: (1) identity theft by the acquiring of 10 or more persons' personal identifying information[27] and (2) acquiring possession of access card information without the permission of the issuer (or cardholder).[28] Other crimes that can be proven with bank and law enforcement witnesses, but might also be accompanied by associated crimes that have an intent to defraud element, include: (1) acquiring four access cards in a 12-month period[29] and (2) false personation.[30] Depending on the facts, other crimes can also fit these categories.

Also, when a prosecutor can prove more than $100,000 in losses, Penal Code section 186.11 allows for powerful tools to levy on a defendant's assets at the time of the filing of the complaint[31] for the purpose of getting restitution.

Charges and Consecutive Sentencing Under Penal Code Section 1170(h)

Even if the sentences do not qualify for state prison, significant sentences can be attained in county jail pursuant to Penal Code section 1170(h), and split sentences can be used to address any drug addiction that is a motivator for the crimes. Consecutive sentences can occur when charges involve separate victims, dates, locations, and intents.[32] Individual counts of identity theft should name specific victims to make it clear that separate victims are involved. Moreover, failure to name victims could negatively affect their ability to be awarded restitution.

If a prosecutor chooses not to use the Penal Code section 786 process, conspiracy charges may be a means to include events occurring in other jurisdictions,[33] but identity theft charges are needed to join other "associated offenses." Similarly, a prosecutor can proceed using the traditional territorial jurisdictional statute with offenses occurring in multiple jurisdictions.[34]

Establishing Jurisdiction in the Filing Court for Multi-jurisdictional Offenses

Currently, there is no case law that specifies the procedure for using Penal Code section 786(b). We look to the plain wording of the statute with guidance being drawn from the procedure a defendant must follow when seeking a change of venue because he or she cannot get a fair and impartial trial. [35] At a minimum, the People's charging document must give notice that there are "charges alleging multiple offenses of unauthorized use of [PII] occurring in multiple jurisdictions."[36] This triggers a requirement that a judge hold a hearing regarding the proper territorial jurisdiction.

Prosecutors will be able to best persuade the court if they file a written motion that alerts the court they are establishing territorial jurisdiction[37] pursuant to Penal Code section 786(b). The motion should provide facts, and points and authorities that show they are complying with Penal Code section 786(b).

The People's motion should be supported by declaration, setting forth the applicable facts. Affidavits should state facts and not mere beliefs or conclusions. The motion should also include evidence that the district attorneys from all counties where the crimes were committed assent to the jurisdiction being set in the court of filing. Except for good cause, the motion must be served on the defendant at least 10 days before the hearing. The defendant has a right to oppose the Penal Code section 786(b) proceeding and file counter declarations at the hearing. In general, the prosecution has the burden of proving proper venue by a preponderance of the evidence. [38]

If the defendant chooses not to oppose, for example in a negotiated plea, the People's motion should be granted or the defendant's waiver of opposition to the jurisdiction should be memorialized by minute order in the docket.

If the defendant opposes jurisdiction being set in the county of filing, then the court in the county of filing shall hold a hearing to consider whether the matter should proceed in that county, or whether one or more counts should be severed. The district attorney filing the complaint shall present evidence to the court that the district attorney in each county where any of the charges could have been filed has agreed that the matter should proceed in the county of filing. This approval should be obtained from the district attorney or the district attorney's designee,[39] in any county where the crime could have been filed. Because this process could implicate double jeopardy issues for the defendant in the assenting district attorney's jurisdiction, it is good practice to provide the assenting district attorney a copy of the Motion to Establish Territorial Jurisdiction and police reports related to the offenses.

As stated in Penal Code section 786(b),

> (2) … In determining whether all counts in the complaint should be joined in one county for prosecution, the court shall consider the location and complexity of the likely evidence, where the majority of the offenses occurred, whether or not the offenses involved substantially similar activity or the same scheme, the rights of the defendant and the people, and the convenience of, or hardship to, the victim and witnesses.[40]
>
> (3) When an action for unauthorized use, retention, or transfer of personal identifying information is filed in the county in which the victim resided at the time the offense was committed, and no other basis for the jurisdiction applies, the court, upon its own motion or the motion of the defendant, shall hold a hearing to determine whether the county of the victim's residence is the proper venue for trial of the case. In ruling on the matter, the court shall consider the rights of the parties, the access of the parties to evidence, the convenience to witnesses, and the interests of justice.[41]

If the defendant is opposing a legitimate consolidation, and a deputy district attorney is concerned that other district attorney's offices might not effectively prosecute severed counts, an effective option is to seek the assistance of deputy attorneys general assigned to the eCrime Unit. They have jurisdiction to handle severed counts in every county in California. Their commitment to prosecute severed counts can be a deterrent to a defense attorney who seeks to sever counts solely to test the will of the People.

CONCLUSION

Penal Code section 786 is an excellent tool for holding an identity thief accountable for multi-jurisdictional crimes. While resources might dictate whether consolidated or separate prosecutions are best, consideration should be given to the strength that is brought by combining prosecutions into one jurisdiction, especially when it leads to proof of the taking of $100,000 or more, or proves the defendant's criminal intent.

Howard A. Wise has been a prosecutor in the Ventura County District Attorney's Office, handling computer crimes and major fraud cases, from 2001 to present. Between 1994 and 2000, at various times, he was the chief prosecutor of the Public Protection Bureau of the Massachusetts Attorney General's Office, an assistant

continued on page 34

MULTI-COUNTY IDENTITY THEFTS from page 33

attorney general, and a special assistant United States attorney. From 1988 to 1994, he was an assistant district attorney in Middlesex County, Massachusetts. In 1999, Mr. Wise wrote the original Massachusetts' Identity Theft statute. He has lectured at the national, state, and local levels on computer crime, fraud, and technology-facilitated sexual exploitation of children, and has developed and taught a college level course on "Legal Aspects of Computer Forensics."

Joe Williams, Jr. started as a prosecutor in Sacramento County in 1995. Previously, he had been a police officer for fourteen years. He joined the Orange County District Attorney's Office in 1999. During the last six years, he has worked in the Major Fraud Unit, specifically targeting Eastern European Crime groups and identity theft rings. To address the transnational crimes caused by these groups, he was also cross-designated as a special assistant United States attorney in the Central District of California. Mr. Williams has also worked with various foreign governments, federal agencies, state agencies, and private sector groups to foster interagency and public-private sector cooperation to help eliminate the impact these criminals have on victims and the public.

ENDNOTES

1. Pen. Code § 786(b).
2. Senate Bill 226, Senate Analysis (June 23, 2009).
3. Skimming can be done in many ways. In general, however, skimmers are devices that are internal or external to the payment device. An internal device is placed inside a gas pump or inside a card reader. An external device is placed over the card reader at an ATM or the locked doorway that allows entrance into the vestibule that holds the ATM.
4. Groups are often organized along ethnic lines with ties to foreign countries. When appropriate, citizenship status should be explored.
5. Pinhole cameras used at banks can be very hard to detect. They can be houses in round "shoulder surfer mirrors" and bars that attach above the ATM. Many Internet sites have pictures of skimmers and cameras.
6. In many other countries, a credit card requires an imbedded "chip." This provides some protection against re-encoded cards.
7. If you can prove knowledge and criminal intent from involvement in other skimmings, "lookouts" can be charged under an aiding and abetting theory or as co-conspirator.
8. Financial Crimes Enforcement Network (FinCEN) reports are often helpful in tracking money and showing a defendant's involvement.
9. Pen. Code § 1275.
10. Pen. Code § 1275.1.
11. Guidance as to the proper foundation and witnesses that need to be laid will likely be given by the California Supreme Court, which has granted review in cases dealing with the admissibility of a traffic light in *People v. Goldsmith* (Carmen) (2012) 203 Cal.App.4th 1515 [review granted and opinion superseded], (Cal. 2012) 280 P.3d 535; and *People v. Khaled* (2012)186 Cal.App.4th Supp.1. See also *People v. Lugashi* (1988) 205 Cal.App.3d 632 [cert. for partial pub.]; *People v. Cohen* (1976) 59 Cal.App.3d 241, 249; and *People v. Dorsey* (1974) 43 Cal.App.3d 953, 960–961.
12. See *People v. Franzen* (2012) 210 Cal.App.4th 1193 (review denied Feb. 13, 2013) [rejecting the admission of certain Internet phone records under the published compilation exception to the hearsay rule].
13. Contact information can be found at the State of California Department of Justice, Office of the Attorney General website <*https://oag.ca.gov/ecrime/httap*> (accessed Nov. 12, 2013).

14. The Eurasian Organized Crime Task Force can be reached at (818) 548-6485.
15. The Los Angeles Fraud Task Force can be reached at (213) 533-4500.
16. The Southern Nevada European Organized Crime Task Force (a.k.a., the Transnational Organized Crime Task Force) can be reached contacting Detective Matthew Jogodka at (702) 828-3019.
17. The SCHTTF can reached at (562) 347-2601.
18. More information can be found at the U.S. Customs and Border Protection website at <*www.cbp.gov.*> CBP includes the agency formerly referred to as ICE. (accessed Nov. 12, 2013).
19. *Sims v. Superior Court of Los Angeles County* (1993) 18 Cal.App.4th 463 [review denied Nov. 24, 1993]. Penal Code section 872(b) applies to officers and agents employed by a federal, state, or local government agency (a) who meet the threshold training and experience requirements set forth in the statute, and (b) whose primary responsibility is to investigate and prepare for prosecution cases involving violations of laws. 4 Witkin, *Cal.Crim.Law 4th* (2012) Pretrial, § 167: 418.
20. For a survey of federal identity theft law see, Martin Richey, AFPD, D. Mass (2010) "Identity Theft." It is written by an assistant federal public defender. See <*http://www.fd.org/docs/select-topics---common-offenses/oct-2010-update-final-x.pdf*> (accessed Nov. 12, 2013).
21. United States Sentencing Commission, *2013 USSC Guidelines Manual*, § 2B1.1(b)(2).
22. Similar language can be found in Penal Code section 186.11(a), which refers to "related felonies, a material element of which is fraud or embezzlement, which involve a pattern of related felony conduct."
23. Pen. Code § 530.5(a).
24. Pen. Code § 1170(h).
25. See Penal Code sections 186.11 and 12022.6 for other particulars that must be pleaded and proved. Because the law is unsettled regarding whether all sections of the identity theft statute (Pen. Code § 530.5) are crimes with fraud as an element, it is good practice to also charge a crime that specifically has fraudulent intent as an element.
26. See *People v. Lai* (2006) 138 Cal.App.4th 1227, 1251[cert. for partial pub.]["when the defendant is sentenced to state prison,… [Penal Code] section 186.11, subdivision (d) authorizes restitution only for losses caused by felonies constituting the 'pattern of related felony conduct' admitted or found true as part of the section 186.11, subdivision (a) allegation"]. See also, the commentary to CALCRIM 3220 for a discussion of what constitutes a loss.
27. Pen. Code § 530.5(c)(3). Although there is no case law on point, because 530.5(c)(3) has an intent to defraud element, it is likely to be a crime included in.
28. Pen. Code § 484e(d). Section 484d(2) defines access code as "any 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."
29. Pen. Code § 484e(b).
30. Pen. Code § 529; *People v. Rathert* (2000) 24 Cal.4th 200, 205–207 [false personation statute is violated when one intentionally falsely personates another and, in such assumed character, does any act that might cause the liability or benefit described in statute, and no requirement exists that defendant must have specific intent to cause described liability or benefit].
31. Pen. Code § 186.11.
32. Pen. Code § 654; 3 Witkin, *Cal.Crim.Law 4th* (2012) Punishment, § 272–277, 289; *People v. Andra* (2007) 156 Cal.App.4th 638, 641[obtaining money by false pretenses and identity theft were divisible crimes].
33. "Conspiracy may be prosecuted and tried in the superior court of any county in which any overt act tending to affect the conspiracy is done." 4 Witkin, *Cal.Crim.Law 4th* (2012) Jury & Ven, § 62: 175.
34. Pen. Code § 781.
35. For a detailed discussion, see, 4 Witkin, *Cal.Crim.Law 4th* (2012) Jury & Ven, § 66–69, 71–72, 181–188; *People v. Parks* (1872) 44 Cal. 105; *People v. Posey* (2004) 32 Cal.4th 193, 213; C.R.C., rule 4.151(a), et seq.
36. Pen. Code § 786(b).
37. "Venue" and "jurisdiction" are sometimes used interchangeably. Venue means the territorial jurisdiction in which a case can be brought to trial.
38. C.R.C., rule 4.151(a) regarding motions for change of venue; C.E.B., *Criminal Law* § 15.17; 4 Witkin, *Cal.Crim. Law 4th* (2012) Jury & Ven, § 72:187.
39. Individual offices have different procedures regarding the person with authority to assent to this process. The process might take time due to busy schedules of top personnel.
40. Pen. Code § 786(b)(2).
41. Pen. Code § 786(b)(3).