

IDENTITY THEFT PREVENTION FOR BUSINESSES

Identity theft related crime has been identified as the fastest growing crime trend in America today. In order to make a positive impact, law enforcement and businesses must coordinate our efforts to better protect ourselves and the citizens we serve.

The home computer has revolutionized the ability of the average criminal to involve themselves in identity related crimes. A large majority of the offenders are being identified as having illegal drug addictions and are utilizing identity theft to further their ability to afford these drugs.

These criminals are stealing mail in order to discover checks (routing and account numbers), credit cards and/or applications (items of mail containing personal information that can be utilized to obtain credit). By using check and ID writing software, offenders are making counterfeit checks and IDs in order to write checks for cash or to purchase retail items.

These suspects are also compromising the credit card industry by obtaining credit cards via the internet application process using stolen personal information. They are also obtaining stolen credit cards through mail theft, burglary from vehicle and other related crimes. Another form of credit card fraud occurs when the offender obtains the credit card numbers from discarded receipts, applications and other paperwork discarded into dumpsters by individuals and businesses.

While advances in technology and the advent of the internet have made it possible for businesses to become more user friendly, it also opened the door for the perpetration of fraudulent activity under cover of anonymity. With the adoption of the below listed business practices you can help to curtail fraud while still presenting a positive user friendly atmosphere for your customers and limit your exposure to civil liability through reckless handling of your customer's personal information.

How to protect your clients/customers

Keep all documents containing personal information of your clients, customers and employees under lock and key.

When personal information is held within a computer, ensure that it can only be accessed and tracked by authorized personnel using passwords and is protected with an appropriate level of security/fire walls. When the information has been transferred to the computer, any handwritten information should be shredded.

Shred customer personal or account information and receipts before discarding them. Consider keeping shredders within reach of those employees who handle personal/account information on a regular basis.

Create policies to restrict the handling of customer information to a limited number of employees.

Customer personal information such as credit applications, sales receipts, or copies should not be temporarily kept within reach of the casual observer. This will help to deter theft by criminals or corrupt employees. Provide a secure receptacle for employees and citizens to throw out applications/receipts or provide informational signs advising them not to carelessly discard these documents.

How to protect your business from fraud

When accepting credit applications or checks, require the applicant to provide a fingerprint directly on the application or check. This is common practice in the banking community and should be readily accepted. This aids law enforcement with identifying exactly who presented the documents.

Install video surveillance in areas where business is conducted with a "loop time" of at least one month. This will allow ample time for the fraud to be detected and the suspect transaction to be pulled for evidence.

Check the orientation, duration and condition of all video surveillance equipment. It is common for video surveillance tapes we review to suffer from one or more of the following problems:

- The camera is oriented improperly (wrong angle, positioned too far away, too wide of a view angle) to accurately resolve the suspect's face. It is generally more important to focus the camera as close to where a customer conducting a transaction's upper body and face would normally be during the transaction. We identify far more suspects from front mounted ATM cameras than we ever do from surveillance videos from businesses for this reason.
- On analog systems, where a form of magnetic media (such as a VHS tape) is used to store the recorded video, make sure to rotate in a brand new video tape a few times a year. Video tapes that are used to continually record, slowly degrade, stretch and lose their magnetic layer. Over time, the video quality from tapes that are not rotated, greatly suffers to the point where it becomes unviewable.
- On digital systems, don't set the compression or time lapse setting too high. At present, hard drive storage is cheap. It is better to have close to real time video of a relatively high quality. For our purposes, we typically get a tape request to businesses in less than a month. Relatively modern equipment should have enough storage capacity to achieve a setting which maximizes video quality and minimizes time lapse, still giving a month's worth of history.
- Make sure that the date and time stamp are set correctly and visible on the tape. If your system does not automatically adjust for daylight savings time, remember to manually make the change.
- Remember, that there are numerous vendors that make digital surveillance equipment. Most use their own proprietary CODEC, or Compressor/De-compressor. This is a file that is needed to make the video viewable by file players such as Windows Media Player, Real Player, etc. It is often not enough to merely copy the video in question onto a CD. We also need either the software player or the CODEC in order to view the file.

Video evidence along with a finger print is very good evidence and reduces the possibility that employees would have to attend court.

Require a photographic ID be presented during check and credit card transactions, along with a fingerprint on the sales receipt and/or check. Inkless pads are cheap and readily available for each register. Debit card transactions utilizing a PIN number need not fall into this category.

If your business retails to other businesses utilizing a business account number and company credit card listed in your computer, understand that this information is often corrupted by ex-employees of the customer business. Always require that your sales representatives call a responsible party with the company to verify the transaction.

If your business accepts telephone or internet orders, always utilize the 3-digit verification number printed on the signature line of the card. This number should not be recorded on the internet order form or receipts generated from sales. This ensures that the card itself is in the possession of the customer and isn't being stolen from a compromised recklessly discarded document.