Identity theft is only the start of a chain of events that ultimately cost victims money. It is not the theft of identity alone that concerns people; rather, it is the financial losses that identity theft enables.

Criminals use victims’ personal information to engage in fraudulent financial transactions that generate cash.

While social engineering, theft of mail, and other nontechnical approaches may sometimes be used to intercept personal data, of bigger concern is the use of technology to copy data from credit and debit cards when they are used in legitimate financial transactions. These data can then be used to create duplicate credit and debit cards, which are then used to drain bank accounts or rack up huge credit card balances.

The criminals who create these “skimming” devices have a high level of technical knowledge. Furthermore, they must install these devices in point-of-sale (POS) terminals or automated teller machines (ATMs) to gain access to victim card data and personal identification numbers (PINs).

Untapped investigative opportunity exists in the seizure of modified POS terminals and ATM overlays. This column examines these opportunities and describes what one Canadian agency, the Vancouver Police Department (VPD), has done to identify these technological criminals and prevent identity theft.

A Technological Approach

A surprising amount of information may be gleaned from forensic examination of recovered electronic devices. This is obvious when seizing computers, cellular telephones, and similar devices. For years these have been examined by forensic experts, and valuable evidence has been recovered.

What is not generally known, however, is that seized ATM skimmers, modified POS terminals, hidden cameras, and similar devices may also yield valuable forensic clues for investigators if the technical details of their construction are properly evaluated.

Aside from the obvious “traditional” forensics such as fingerprints and DNA that can be recovered from such devices, the actual construction of the units or the modifications themselves may yield a surprisingly large amount of useful information for investigators. This evidence or knowledge might lead investigators to a successful conclusion of the case. Some examples follow:

- Circuit boards that hold the electronic components for “skimming” devices (the material on which parasitic microprocessors and other parts are mounted) often have a fabricator’s name or logo silk-screened onto the board. Criminals who mass-produce these boards will often go to a commercial circuit board fabricator for this work. Commonly, the fabricator will include its logo, company name, and most importantly a “run number” or “order number” on the board. This can lead investigators to suspects.

- All integrated circuits and microprocessors as well as some other components have manufacturing codes printed on them. An electronics professional will be able to interpret these codes to determine date and location of manufacture for the part. From these codes it may be possible to determine where the part was sold using a list of suppliers. These can help investigators locate the specific supplier of the part, again leading to suspects, as some of the parts used in skimming and overlay devices are not all that common.

- To the trained electronics professional, the way the circuit is physically laid out on the circuit board, and the method that the circuit uses to “solve” the problem of intercepting victims’ keypad codes, for example, is highly indicative of the demographics of the suspects. Experienced engineers will be able to examine the seized skimming device, look at the parasitic circuit boards and components, and determine the level of the suspects’ education, their background in general, and clues to where they obtained that education.

Source: From The Police Chief, vol. LXXV, no. 4, April 2008. Copyright held by the International Association of Chiefs of Police, 515 North Washington Street, Alexandria, VA 22314 USA.
Electronic and computer professionals can assist investigators in another way as well. Skimming devices are constructed around microcontrollers—miniature computers on a chip. Computers need software (in this case called “firmware”) in order to run. The firmware stored within these systems serves to do the work of intercepting and storing customer data for later retrieval by the suspects. This firmware may be retrieved from the device by electronics and computer system professionals and examined for clues as to its originators. As with the physical hardware, the style and efficiency of the firmware can tell investigators a lot about the suspects.

All this sounds very technical. Agency leaders may wonder how they can convince investigators to consider these factors when they seize a skimming device or ATM overlay. Indeed, examination of seized POS and overlay devices at this technical level is beyond the skill level of most police officers. This is a fact, but it can be addressed most effectively through collaboration with the high-tech industry.

Collaboration with Industry

Last year, detectives in the VPD Financial Crime Unit conducted an investigation into payment card skimming at local restaurants and business establishments. Among other items, two modified POS terminals were seized (see photo on page 20). Up to this point, the unit had no information on the suspects.

The investigators were unaware at that time of the large amount of forensic evidence that could be recovered from these compromised devices. Discussion of the case in the office led the unit to consider an innovative idea for gathering intelligence on the suspects.

Through contacts in the local high-tech industry, investigators were able to meet with a senior electronics engineer at a major wireless-systems design firm. With some 30 years of experience in the design, fabrication, and troubleshooting of electronics and circuitry of all types, this individual was intrigued by the opportunity to assist the police in the investigation of the case. He volunteered his services, and the investigators met with him to transfer the modified POS devices and give him some background on the case.

The collaborator dove into the case with a lot of enthusiasm and, over the following two weeks, completed a very detailed report on how the additional circuitry had been connected into existing circuitry of the POS terminals. The report eventually stabilized at 85 pages and provided a comprehensive analysis of the modifications and what could be learned from them about the suspects.

This information has been of incredible value to the investigators and has opened up several new leads, both in this case and in a general sense by pointing toward the group of suspects who are responsible for this particular “line” of parasitic circuitry. The Financial Crime Unit has now successfully concluded its investigation, which spawned another investigation into the suspects’ tech crime activities that span Canada and have tentacles reaching into both Europe and the United States.
Results of Analysis

Analysis of the seized POS devices produced several interesting facts and observations.

**Device:** In the expert’s opinion, the POS terminal has poorly designed security features that may be easily defeated. Improvements in the design of the POS terminal could make criminal modification much more difficult.

**Parasitic Hardware:** The expert described the suspects’ techniques as “crude but highly effective.” Two circuit boards, one magnetic stripe reader, a custom-manufactured flexible membrane keyboard, and one battery were added to the stock POS device. This new circuitry interconnects with the POS terminal and draws power from it. The battery is used to maintain the skimmed customer data in memory for later retrieval. Between 1,000 and 4,000 sets of victim data could be stored.

Parts used in the modifications are generally available at many outlets, but notably, two critical components of the modification were manufactured in a particular major city in Canada; one of these components is quite sophisticated and unique. This information alone moved the investigation forward.

**Software:** The software (firmware) used to program the microcontroller on the parasitic circuit board was likely based on publicly available programs found on the Internet. These programs are provided by the manufacturer of the microcontroller and are not inherently designed for criminal purposes. The suspects likely modified this general purpose programming code for use in their illegal activity. A higher technological skill level is required to develop or customize this software than to assemble the parasitic components themselves.

**Suspects:** The expert described the suspects as creative and intelligent, having fair, basic knowledge of electronics and building techniques but lacking consistency and discipline. Although they followed standard electronics practices for some parts of the modifications, they ignored others.

The suspects likely followed a “recipe” for the modifications rather than truly understanding why certain modifications needed to be made to the POS device. Some aspects of their modifications to the original POS circuitry did not make sense from the point of view of a technically qualified expert.

The suspects removed the serial number from one key part in the modification but not from other parts. This is indicative of their lack of discipline as noted.

The design of a critical component of the modification (the membrane keypad used to capture victims’ PIN data) is closely tied to the success of the overall modifications. This component is pivotal to the modifications, unique and specially designed for this particular application, and could only be fabricated at a few shops in Canada. The “Made in Canada” stamp, logo, and batch number on the membrane proved of great value in the investigation.

The programming skills necessary to develop the software (firmware) for the microcontroller indicate an education at the technical-school level or higher, with some actual experience in industry. The expert’s opinion was that the suspects likely have a hobby background in electronics.
Conclusion and Recommendations

Although this column has focused on forensic analysis and reverse engineering of a modified POS terminal, these techniques have equal application to ATM overlays, hidden-camera installations, listening devices, and customized or modified electronic devices of all types.

Through this innovative approach, the VPD has been able to expand the scope of this skimming investigation. Additionally, through its collaborative work with the high-tech industry, the forensic analysis of the seized POS terminal exposed previously unknown technological details of the crime and the logistics of how it was perpetrated. Through this analysis, the Financial Crime Unit also learned a lot about the background of the suspects.

The intelligence gained through expert consultation and analysis has led the unit to a well organized group of suspects who it believes are responsible for a significant percentage of skimming activity in Canada. Working with partner police agencies, the unit hopes to obtain further insight into the suspects’ activities, shut them down, and help eradicate this type of crime.

With the recent huge increase in technological crime, police cannot be expected to keep abreast of all the newest technologies and how criminals may leverage them for personal gain. Partnerships with experts in the high-tech industry can address these gaps. Companies will often provide this assistance free of charge, as they are also members of the community; even senior executives have been victimized by tech crime and identity theft. Assisting the police in an active investigation is also of interest to many high-tech employees - it gives them something different to do that is far removed from the high-pressure development and production cycles that are the norm within most high-tech firms.

In the case described here, the VPD acknowledged the assistance of the expert collaborator and his company by presenting them with a plaque recognizing their contributions to the investigation and thanking them for their assistance. The CEO of the firm accepted this award with pride, as one of his company’s objectives is to be supportive of the community and its employees in their community-oriented activities. With this relationship in place, the department will continue to work with the firm and this expert as needed.

Outside of the framework of a particular investigation, all police officers working in technological crime areas can benefit greatly from these industrial relationships. The VPD is developing similar relationships with other industries to mutually augment or complement technological and investigative capabilities. In some cases, relationships with high-tech experts have even developed into friendships and social relationships, in which both parties benefit greatly from the other’s skills and expertise. This is community policing at its best.

Encourage your tech-crime investigators to establish relationships with local high-tech firms. Send your officers to high-tech conferences and seminars. Build contacts in the engineering and computer science faculties at your local colleges. Your investigators will improve their technical skills and learn a lot about new technologies, which will result in more successful investigations.

The VPD acknowledges the assistance of Sierra Wireless, Inc., of Richmond, British Columbia, and Peter McConnell (P.Eng.) for their assistance. Without their support, the VPD could not have successfully concluded this investigation.

For more information, contact the author via e-mail at kevin@vpd.ca.

From The Police Chief, vol. LXXV, no. 4, April 2008. Copyright held by the International Association of Chiefs of Police, 515 North Washington Street, Alexandria, VA 22314 USA.