Green Dot MoneyPak Fraud Schemes
Green Dot MoneyPak Fraud Schemes

A caller threatens to detonate an explosive device inside a drugstore in Louisiana unless money is wired to him. A fraudster claiming to be from the power company tries to extort a homeowner in Virginia. A prison gang in Maryland laundered its extortion proceeds. Mexican drug cartels move money effortlessly across the border.

The only connection among these examples of criminal activity is the use by the perpetrators of prepaid reloadable debit cards to facilitate their payoff. The cards can also be used by criminal organizations to launder illegal proceeds and move funds across borders. They are called General Purpose Reloadable (GPR) or Prepaid and Stored Value (PPSV) cards and are marketed to persons who don’t want to use or can’t afford to use a traditional bricks-and-mortar bank. No credit check is needed to purchase a prepaid card.

A large majority of these fraudulent activities specify the use of Green Dot cards and Green Dot MoneyPaks because Green Dot is one of the most popular brands of prepaid or value-stored cards in the U.S. However, there are many card brands out there—AAA, American Express Bluebird, Blackhawk, MoneyGram, Target, and Walmart just to name a few—some with very specific target audiences and legitimate uses.

Gift cards and phone cards are single-load or closed-system debit cards, usually usable only with certain merchants. Green Dot and similar cards are “open-system” cards, usable at thousands of businesses across the U.S. and able to be

(Continued on Page 3)
Prepaid and Stored Value Cards

- American Express
- AAA
- Blackhawk PayPower
- H&R Block Emerald
- MoneyGram
- netSpend
- Travelex
- Target
- Walmart
- Western Union MoneyWise
reloaded with value. If they’re “branded” cards — if they come with the Visa or MasterCard logo — they can be used to withdraw money directly through ATMs.

The explosive growth in the use of prepaid cards by consumers in recent years has resulted in a multi-billion dollar prepaid card industry, according to the Financial Crimes Enforcement Network (FinCEN) of the U.S. Treasury Dept.

Law enforcement and regulators say that scams where fraudsters receive payment through Green Dot, the nation’s leading provider of prepaid debit cards, are spreading across the country as its reloadable MoneyPaks replace more traditional wires from Western Union and MoneyGram.

Thieves are favoring Green Dot and other prepaid cards because MoneyGram, which settled charges with the Federal Trade Commission in 2009 regarding oversight of telemarketing fraud, and Western Union now have sophisticated fraud detection programs and electronic transaction flagging systems, said Steven Baker, a fraud expert with the FTC.

Green Dot prepaid debit cards are available at approximately 60,000 retail outlets throughout the U.S. and are reloadable through the purchase of MoneyPaks, which carry a unique authorization number. These cards are not associated with any personal bank account. Users of these Green Dot MoneyPak cards are reminded to never give anyone those numbers associated with those cards — doing so gives them instant access to the money on those cards.

Green Dot Corporation, headquartered in Pasadena, Calif., works closely with law enforcement in combatting fraud (see page 15 for details), stated Senior Vice President Jeff Ross, who had 32 years of law enforcement experience before coming to Green Dot in 2008. He was a money laundering expert at the Department of Treasury after serving 19 years in the US DOJ Criminal Division specializing in counter-money-laundering policies. He noted that law enforcement can subpoena all details of card activity from Green Dot, not a single transaction detail is excluded. Turnaround time for a request is usually the same day.

Prepaid cards function like traditional checking account debit cards, without the checks. A MoneyPak comes with a scratch-off 14-digit serial number. To transfer funds to a prepaid debit card, holders call or visit the MoneyPak or Green Dot websites and reveal the number. Once fraudsters have the code, they can then transfer the funds to their own prepaid debit cards, typically opened under stolen identities, to make purchases or withdrawals from ATMs.

Customers can load up to $1,000 a day on MoneyPaks for $5.95 per transaction, and get cards with a number on the back. The cash is
held by Green Dot’s partner banks and accessed through the number, similar to a bank account’s routing number. Green Dot cards are not sold outside the U.S. and cannot be reloaded from abroad. MoneyPaks are often used to fund PayPal accounts, which are used to make payments on the Internet.

**Scammers calling in bomb threats**

The FBI and the St. Charles Parish, La. Sheriff’s Office are investigating a series of telephonic threats that occurred Sept. 17, 2013, from an unidentified Asian male who called CVS stores in Destrehan, Ponchatoula, Covington, and Mandeville, all in Louisiana.

The caller demanded Green Dot cards be activated, loaded with $500 and the security number on the back provided to him or he would detonate an explosive device previously placed inside the store.

Similar incidents occurred Sept. 16, 2013 in the Lafayette, La. area. Calls were placed to CVS and Walgreens stores in New Iberia, St. Martinville, Youngsville, and two calls in Lafayette, all in Louisiana. No explosive devices were found in any of the incidents.

A similar scam was reported at Kmart, Walgreens, and CVS stores in Virginia and New Jersey. On Aug. 31, 2013, a subject with a Middle Eastern accent stated his name (unintelligible) and said, “I’m calling from Pakistan and I need to speak to your manager.” Once the manager was on the phone, the male subject stated, “This is (unintelligible) there is a bomb in your state. I know the address of your family so do as I say. It has to stay between you and me. Go grab three Green Dot cards and put $500 on each of them.”

The FBI Atlanta Division issued an alert on Sept. 16, 2013 warning consumers of Green Dot MoneyPak scams in Georgia. These scams were conducted in the same manner.

On Sept. 12, 2013, ten retail stores in Savannah, Ga., each received telephonic bomb threats. In each case, the caller asked to speak to the store manager, demanding that ten Green Dot MoneyPak cards be activated and loaded with $500 and that the card numbers be read aloud over the phone. The caller threatened to blow up the stores if the managers did not comply and also threatened the store employees’ homes and families.

The managers of all the stores described the caller as a male between 20 to 30 years of age and with a foreign accent. No manager complied with the demands, and no explosive devices were found.

Subsequent investigation has determined that these calls mirrored a number of similar telephonic threats made to various drug stores and retail outlets nationwide. One such call placed to a discount department store in Snellville, Ga., was identified as an overseas Voiceover IP (VoIP) telephone number. To date, no explosive devices have been found anywhere in the country linked to this type of threat.

Ross of Green Dot said many of the phone threats have been traced to major phone numbers in India (Indians in the U.S. are also targeted).

**Stolen cards altered, replaced at store**

In December 2013 in Atlanta, Ga. a group of thieves perpetrated a new scheme involving Green Dot cards, according to the FBI. They would steal the cards at the store, remove the seal on the back to reveal the account number, and link the account number to a debit card. They

(Continued on Page 6)
How Do Green Dot Prepaid Cards Work?

When a customer purchases a Green Dot prepaid card, he or she initially receives a temporary card from the retailer where the card was sold. At the time of purchase, consumers usually add (or “load”) funds to a given card. For example, a consumer may purchase a temporary card and, at the time of purchase, request that a certain amount, for example, $100, be loaded onto the card. The maximum that may be loaded to a Green Dot temporary card is $500.

Before a temporary Green Dot prepaid card can be used by the cardholder, the cardholder must contact Green Dot, either through the website or the Green Dot call center, in order to activate the card. Card activation includes a cardholder registering the card in addition to the cardholder providing certain personal identifying information that is verified by Green Dot. Once that process is complete, the non-personalized, non-reloadable temporary card is activated.

Green Dot submits the collected information (e.g., name, SSN, DOB, address, and phone number) for verification to third party vendors. Foreign identifications and other non-SSN identification data are not accepted by Green Dot. According to Green Dot, as part of verifying a cardholder, the identifying information collected from the cardholder is also processed through an automated system that queries the cardholder’s name, as well as the name of any secondary cardholders, against the Specially Designated Nationals (SDN) list that is maintained by the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC). Green Dot also queries new cardholders within its own internal systems that contain the names of previous Green Dot cardholders whose card(s) were previously closed by Green Dot due to violations of Green Dot’s user agreement or for other business reasons.

If the customer passes Green Dot’s customer verification process, Green Dot will then send a personalized reloadable card in the mail embossed with the cardholder’s name. Once the customer receives the personalized card, he or she must register the card by contacting Green Dot through the website or the call center. The funds from the temporary card will be transferred to the personalized card once the customer registers the personalized card or 30 days after the activation of the temporary card, whichever occurs first.

As part of activating a Green Dot prepaid card, the cardholder must also establish a four-digit Personal Identification Number (PIN) that will be used for PIN-based transactions and ATM cash withdrawals. Additionally, if the cardholder is activating his or her temporary prepaid card via the Green Dot website, he or she must also provide Green Dot with an email address. If a cardholder purchases additional Green Dot temporary cards, he or she is required to re-initiate the same activation process noted above with each card.

Once a Green Dot prepaid card has been activated, the cardholder can use the card at any merchant or business (including online merchants) where Visa or MasterCard debit cards are accepted. There are numerous transaction modes, including the card being swiped through a merchant’s point-of-sale equipment, customer PIN and signature-based transactions, website and phone-based transactions, and ATM withdrawals.

After spending funds on a Green Dot prepaid card, the cardholder may choose to reload funds onto the card. There are several ways to reload the card, including swiping it on-site at Green Dot retail partner locations, receiving pay via a direct deposit, using the aforementioned Green Dot MoneyPak, or via an electronic funds transfer from the cardholder’s external bank account via use of the Automated Clearing House (ACH).

replace the seal on the card to make it appear unblemished and return it to the store. Once a customer purchases the card, the money is then wired to the debit card account. The perpetrator will continually check the stolen cards’ account balance by phone or computer to identify changes on the stolen cards. As this scam became prevalent in the metro Atlanta area, stores began to place the cards behind the counter to limit access. The suspects then moved their operation outside of Atlanta into areas unfamiliar with this scheme, including Athens, Ga. The suspects would often use the money from the scheme to buy illegal narcotics and would resell them to make a larger profit.

Ross of Green Dot called this scheme “really insidious.” If alerted, Green Dot can monitor the card number to see if fraudsters are pinging on it (to determine when it is activated) and then deactivate it, if necessary.

**Counterfeit receipt used for refunds**

In May 2013 at a Walmart in Naples, Fla., a white female used a counterfeit receipt to obtain refunds totaling $887 on Green Dot cards, according to the Collier County Sheriff’s Office. Numerous Walmart locations throughout the U.S. have experienced this scam, with losses totaling $395,764.

**Scammers only need a number**

In January 2013, an employee at the CVS pharmacy in Auburn, Ala. complied with a caller claiming to be a CVS corporate executive investigating a virus threat. The night-shift employee was persuaded to run a transaction to reload prepaid cards that resulted in a loss exceeding $10,000.

An unidentified suspect using the name Bobby Johnston called at least five Herndon, Va. residents claiming to be with Dominion Power electric company. He claims that the victim owes money ($1,400 to $1,500) and immediate payment must be made to continue service. The suspect instructs the victim to buy Green Dot cards or MoneyPaks in increments of $500 at CVS, Walgreens, or similar stores. The victim calls Johnston back with the account numbers and the money is transferred out of the account.

Phone fraudsters are using the threat of arrest warrants to pressure people into forking over hundreds, sometimes thousands, of dollars. In August 2013, police in Florida, Georgia, Kansas, and Oregon investigated phone scams in which a caller impersonates a local police officer. The callers, manipulating caller ID to make the number appear to come from the local sheriff’s office or jail, tell potential victims they have an outstanding warrant for an unpaid debt, missed jury duty or some minor infraction and that a fine is due. The callers convince people to make the payments by wiring it through Western Union or buying a prepaid credit card like Green Dot and registering it online.

Police don’t notify people about arrest warrants by phone, and they don’t accept money to clear them, the Collier County, Fla., sheriff’s office stated.

“They try to make this as convincing and as frightening as possible,” says Kati Daffan, a staff attorney with the Federal Trade Commission’s Bureau of Consumer Protection.

In Georgia’s Floyd County, a 31-year-old woman paid $1,550 to clear a non-existent arrest warrant related to a payday loan she never had. She received a call saying she owed $495 for a loan. She says she checked with her creditors and found no record of the loan. She had previous debt disputes after another person of the same name failed to pay off a loan, she said, so she brushed it off and...
told the caller to email proof. But after a second call from a so-called police officer threatening to arrest her, she gave in.

“He said, ‘In our eyes, you’re just refusing to pay the debt,’” she recalled. “We’re just going to have to proceed forward and have you arrested.”

Her husband checked the number; it was the sheriff’s office. She paid the $495, along with a $500 fine and several “litigation fees” — a total of $1,550. Only after she sent the money through a prepaid credit card did she call the sheriff’s office and learn there was no warrant.

In Tuscaloosa, Ala., elderly residents have been called by a fraudster claiming to be a lieutenant with the local police department. He persuades the victim to purchase a $498 Green Dot card to pay off a red-light camera traffic ticket. Once the suspect gets the card number, he can download the money to his own card. The suspect calls the victims by name and in one case correctly identified their vehicle and tag number.

A resident of Coconut Creek, Fla. became suspicious when a caller claiming to be from Publishers Clearinghouse sweepstakes told him he had just won $50,000, but he first needed to pay $191 in processing fees through a prepaid card he could buy at Walmart. When he hesitated, the caller “gave me a hard time, and told me to think of all the things I could do for other people with the money,” he said. “That’s when I hung up.”

The Better Business Bureau in St. Louis, Mo. issued an alert when more than 40 unsuspecting borrowers lost tens of thousands of dollars when they sent financing charges on MoneyPaks. The FTC said thieves running lottery and sweepstakes scams, where more than 40 percent of the victims are over age 70, now often ask for MoneyPak payments.

“If you are going to run a scam, you need a way to collect the money,” said Steven Baker of the FTC.

**Thieves impersonate officials**

In April 2013 in Sioux Falls, S.D., a female suspect went to Walmart and requested six Green Dot cards be loaded with $1,000 each, then left the store without paying. She claimed to be from the main office and was running a test to see how long it took to load the cards, according to the South Dakota Fusion Center. The suspect, along with a white female accomplice, have hit several Walmart stores in Arkansas, Kansas, Missouri, Nebraska, Minnesota, and South Dakota. The Green Dot scams started in September 2012 and continue to be reported.

**Beware the crooked tax man**

Crooks posing as IRS agents, and who somehow know the last four digits of your Social Security number, claim you owe back taxes that must be immediately paid via a Green Dot MoneyPak.

If you refuse to cooperate, you’re threatened with arrest, deportation or suspension of a business or driver’s license. The scammers also spoof an IRS toll-free phone number on your Caller ID, give IRS badge numbers, and follow up their calls with emails purporting to be from the agency. The scammers may become hostile, and then hang up – and another person quickly calls back claiming to be from the local police or Department of Motor Vehicles office.

“If someone unexpectedly calls claiming to be from the IRS and threatens police arrest, deportation or license revocation if you don’t pay immediately, that is a sign that it really isn’t the IRS calling,” said an IRS official.

In 2011, the U.S. Secret Service conducted Operation Rainmaker in Tampa, Fla. and busted sus-
pects who were using laptop computers to steal taxpayer identities and claim tax refunds from the IRS and have the funds directly deposited onto prepaid debit cards. Classes, often thrown as parties, were held to teach street-level offenders how to work the scheme. Defendants told authorities that the computer scheme was much more convenient and safer for them than working scams and thefts on the streets.

**Internet scam locks up computers**

“We’re getting inundated with complaints,” said Donna Gregory of the Internet Crime Complaint Center (IC3), referring to the virus known as Reveton ransomware, which is designed to extort money via prepaid cards from its victims.

Reveton is described as drive-by malware because unlike many viruses—which activate when users open a file or attachment—this one can install itself when users simply click on a compromised website. Once infected, the victim’s computer immediately locks, and the monitor displays a screen stating there has been a violation of federal law.

The bogus message goes on to say that the user’s Internet address was identified by the FBI or the Department of Justice’s Computer Crime and Intellectual Property Section as having been associated with child pornography sites or other illegal online activity. To unlock their machines, users are required to pay a fine using a prepaid money card service.

The Reveton virus, used by hackers in conjunction with Citadel malware—a software delivery platform that can disseminate various kinds of computer viruses—first came to the attention of the FBI in 2011. The IC3 issued a warning on its website in May 2012. Since that time, the virus has become more widespread. Some variants of

---

**TARGETING THE ELDERLY**

Scammers know what we want: to feel secure, loved and valued. And they know that the older we get, the more we need peace of mind. To provide it, some use sweet talk, promising a solution to a problem: money for our shrinking nest eggs, companionship for our lonely hearts, a chance to show we matter. Others feign a problem that needs quick solving, perhaps with some warning about a potential danger.

“The scammer’s goal is to get you to not think rationally, to operate on an emotional level,” says Jean Mathisen, director of AARP’s Fraud Fighter hotline (800-646-2283), which provides counseling, education and victim advocacy. “To put you ‘under the ether,’ as it’s called.”

Some of the come-ons:

*Congratulations, sir. We’re sending you a free medical alert device. Now you can relax about your safety.*

*I know you love me, Grandma. Please send the money so I can get out of jail. I want to come home.*

*Maybe others don’t care about you, but I do. I’ll listen.*

The natural aging process can cause changes in brain function that benefit scammers. Often subtle, even unnoticeable, these shifts often occur around the mid-60s.

At this age, the processing of information slows. This can make you more likely to fall for scams urging you to act immediately.

Age-related brain changes can hamper the ability to recognize facial expressions that signal deceit.

Lies repeated again and again are more likely to be perceived as true as you age, experts say. Con artists use tactics that rely on an erosion of memory or the ability to focus attention.

—AARP Bulletin Jan./Feb. 2014, by Sid Kirchheimer
Reveton can even turn on computer webcams and display the victim’s picture on the frozen screen.

“We are getting dozens of complaints every day,” Gregory said, noting that there is no easy fix if your computer becomes infected. “Unlike other viruses,” she explained, “Reveton freezes your computer and stops it in its tracks. And the average user will not be able to easily remove the malware.”

Be aware that even if you are able to unfreeze your computer on your own, the malware may still operate in the background. Certain types of malware have been known to capture personal information such as user names, passwords, and credit card numbers through embedded keystroke logging programs.

Money laundering concerns
The U.S. would seem to be especially vulnerable, because it’s the world’s biggest user of prepaid cards; the FATF report projected that by 2017, the U.S. will account for 53 percent of the worldwide market.

In congressional testimony last year, FBI Director Robert Mueller called the use of prepaid cards a “shadow banking system” that had “impacted our ability to gather real-time financial intelligence.”

The Financial Crimes Enforcement Network (FinCEN) of the U.S. Treasury Department is tasked with combatting money laundering and promoting the security of financial institutions and transactions. It is responsible for enforcing the Bank Secrecy Act, for example.

The FinCEN Director told Congress in June 2012: “Under FinCEN’s regulation, non-bank providers of prepaid access are now subject to comprehensive requirements similar to depository in-

**MONEY LAUNDERING**
allows criminals to infuse illegal money into the stream of commerce, thus manipulating financial institutions to facilitate the concealing of criminal proceeds; this provides the criminals with unwarranted economic power. The FBI investigates money laundering cases by identifying the process by which criminals conceal or disguise the proceeds of their crimes or convert those proceeds into goods and services. The major threats in this area stem from emerging technologies, such as stored value devices, as well as from shell corporations, which are used to conceal the ownership of funds being moved through financial institutions and international commerce. Recent money laundering investigations have revealed a trend on the part of criminals to use stored value devices, such as prepaid gift cards and reloadable debit cards, in order to move criminal proceeds. This has created a “shadow” banking system, allowing criminals to exploit existing vulnerabilities in the reporting requirements that are imposed on financial institutions and international travelers. This has impacted our ability to gather real time financial intelligence, which is ordinarily available through Bank Secrecy Act filings. Law enforcement relies on this intelligence to identify potential money launderers and terrorist financiers by spotting patterns in the transactions conducted by them. The void caused by the largely unregulated stored-value card industry deprives us of the means to collect this vital intelligence. Moreover, stored value cards are often used to facilitate identity theft. For example, a criminal who successfully infiltrates a bank account can easily purchase stored-value cards and then spend or sell them. This readily available outlet makes it much more unlikely that the stolen funds will ever be recovered, thus costing financial institutions and their insurers billions of dollars each year.

stitutions. The final regulation reflects FinCEN’s attempts to achieve the right balance. FinCEN believes that certain prepaid programs operate in such a way as to reduce potential money laundering threats and are therefore generally not subject to the provisions of the regulation. Such products include payroll cards, government benefits cards, health care access cards, closed loop cards, and low dollar products with strong safeguards in place.

In an examination of the threat, the Financial Action Task Force, an international agency established by the G-7 in 1989, said such an operation typically works like this:

A criminal organization repeatedly loads a prepaid card in increments just below the amount that would trigger a report to the government. (In the U.S., that threshold is $10,000, so if it were based here, the organization might regularly reload a card with $9,900.) Green Dot limits transactions on cards to $2,000. In December 2013 alone, Green Dot filed 943 Suspicious Activity Reports (SAR) involving $10.7 million.

The card, or a second card linked to the same account, is sent to an associate, perhaps in another country, who withdraws the funds through ATMs. In one such operation based in Australia, more than $100,000 was laundered this way, the FATF reported.

That’s how the Black Guerrilla Family, a Baltimore street gang, worked, according to a federal racketeering indictment. For more than a decade, gang members locked up in Maryland’s prisons blackmailed fellow inmates and sold narcotics and other contraband, the FBI said. They then “launched the proceeds of their illicit activities through the use of prepaid debit cards” sold by Green Dot, the nation’s largest seller of the cards in retail stores.

**Conclusion**

Educating the public about the proper use of prepaid cards and the various types of scams being perpetrated by fraudsters may be the most effective strategy for defeating such schemes but law enforcement should be alert to the indicators and how to recognize such offenses in progress.

If the thought of consumers getting ripped off by fraudsters via use of prepaid cash cards doesn’t raise any red flags for you, consider this scenario, as posed by a Treasury Department assessment of financial security threats in 2005:

“The money men behind the Sept. 11, 2001, hijackers would never have been identified had they not been lousy bankers. The 9/11 hijackers opened U.S. bank accounts, had face-to-face dealings with bank employees, signed signature cards and received wire transfers, all of which left financial footprints. Law enforcement was able to follow the trail, identify the hijackers and trace them back to their terror cells and confederates abroad. Had the 9/11 terrorists used prepaid … cards to cover their expenses, none of these financial footprints would have been available.”
Common Consumer Scams Using Prepaid Cards

Advance Payment Scams
These scams come in many varieties and are identified by the need to pay money to get money. The following three common variations can be avoided by remembering that you should not have to pay money to claim something you won or to obtain a loan.

(1) Grants: You receive a check for a few hundred or even a thousand dollars with a communication congratulating you for being awarded a $10,000 grant from Green Dot. The instructions indicate that to collect the rest of your “grant,” you must pay commissions by depositing the check, purchasing MoneyPak cards for the amount of the check, and sending your contact the numbers for MoneyPak purchases. The check is fake, but the money you used to purchase the MoneyPak cards is real. The grant never comes through; the legitimate company did not authorize the grant and will not reimburse you for your loss. You owe the bank the full amount of the check.

(2) Loans: A “lender” informs you that you are pre-approved to apply for a personal loan. Before you get the money, you need to show your ability to repay the loan by making the first two payments. You are instructed to buy a MoneyPak to cover the first two payments and give the “lender” your MoneyPak numbers. The loan never comes through, and the “lender” cannot be traced.

(3) Lotteries or Sweepstakes: You enter lots of lotteries and sweepstakes, and you finally get a notice that you won! To collect your winnings, you have to pay fees or taxes - right away. Rather than sending a check or wiring the fees and taxes (also bad ideas), you are instructed to buy a MoneyPak for the identified amount and simply send the numbers. You pay the amount, but you never get your money. You will be placed on a “suckers” list and receive more bogus offers.

Auction/Sale Scams
An ad for goods or services requires payment using MoneyPak. You provide the requested numbers or receipt information, but the goods or services don’t come. The seller is unreachable.

FBI or Other Law Enforcement Internet Scams
While surfing the Internet, your screen locks up with a message pretending to be from the FBI or another law enforcement agency. The message states that there has been a violation of law punishable by fines and penalties and directs you to pay them using a MoneyPak immediately or criminal charges will be filed and your computer will remain locked. You follow the instructions and pay using a MoneyPak. Your computer may or may not remain locked.

Imposter Scams
You get an urgent call or email from someone who claims to be a relative, friend, law enforcement officer, medical provider, government employee, or any other individual likely to get
Common Consumer Scams Using Prepaid Cards

your attention. The convincing imposter claims to need the money to help your relative or friend who is traveling in another country. The imposter says the best way to help is to purchase a MoneyPak and give them the numbers.

**Job Scams**
You have been applying for many jobs, and you finally get an offer. The company wants you to send money in advance to pay for a background check, uniform, or equipment. You are instructed to purchase MoneyPak cards to pay, and you provide the required numbers, but the job never materializes.

**Romance Scams**
You have been communicating with someone, and things start getting serious. You feel good about the relationship, and your significant other tells you that he or she needs money by way of a MoneyPak card to visit you, to move for a new job, or some other “legitimate” expense. You send the money, and either you do not hear from that person again, or you hear more about other urgent needs.

**Utility Scams**
A caller claims to be from a utility provider, and the caller-ID verifies the source of the call. The caller threatens customers with disconnecting service to their home or business if they fail to make an immediate payment using a MoneyPak card. The caller-ID is falsified, and any payments made will not go to the utility provider and cannot be traced. If you receive a suspicious call that claims to be from a utility provider, end the call and contact the utility provider at the number listed on your bill. Utilities have a variety of payment options available for customers, including the ability to pay over a secure Internet site; by U.S. mail; in person at an authorized pay agent location; or by Visa, MasterCard, or an eCheck using an authorized utility agent.
7 Consumer Tips to Prevent Fraud:

- Never give your MoneyPak number to someone you don’t know.

- Never give receipt information about your MoneyPak purchase to another party.

- Use your MoneyPak only to reload your prepaid cards or accounts you control.

- Refuse any offer that asks you to buy a MoneyPak and share the number or receipt information by email or phone.

- To use your MoneyPak with PayPal or eBay or other online merchants, transfer the money to your PayPal account before you pay the merchant. Don’t email your MoneyPak number directly to any merchant.

- Don’t use the MoneyPak to pay taxes or fees to claim “winnings” on a foreign lottery or prize promotion. Unless it’s an approved MoneyPak partner, don’t use MoneyPak for any offer that requires you to pay before you get the item.

- Check the list (online) of approved MoneyPak partners before you use your MoneyPak to pay.

Please keep these tips in mind when using MoneyPak. Green Dot is not responsible for the quality or non-receipt of any goods or services you buy using your MoneyPak.

Source: https://www.moneypak.com/ProtectYourMoney.aspx
<table>
<thead>
<tr>
<th>Card Programs</th>
<th>Characteristics</th>
<th>Target Market</th>
<th>Possible Issuer Benefit</th>
<th>Potential Threat</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gift cards and prepaid phone service (Single service provider)</td>
<td>Store- or brand-specific (No payment network branding) Cards often sold in pre-set denominations. Merchant collects full value upfront</td>
<td>High frequency customers</td>
<td>Float, increased sales</td>
<td>BMPE-style ML exchanging cash for cards. Use as alternative currency. Distribution method is cash intensive creating ML threat</td>
<td>Retailer-specific and phone service cards</td>
</tr>
<tr>
<td>Gift cards: Multiple Merchants</td>
<td>Multi-mechant gift card; can be used for purchases only (no ATM). Can be payment network branded</td>
<td>Gift givers</td>
<td>Float, sales, and transaction fees</td>
<td>Money laundering through bulk card acquisition and resale</td>
<td>Mall card</td>
</tr>
<tr>
<td>Payroll cards</td>
<td>Creates account to facilitate direct deposit. Cards can be used at ATM and POS</td>
<td>Unbanked workers who are being paid by cash or check</td>
<td>Fee income (lower cost to employer)</td>
<td>Fraudulent businesses could use to pay terrorists or launder money</td>
<td>Various</td>
</tr>
<tr>
<td>Remittance cards</td>
<td>Cards are issued for friends &amp; family to use at cross-border ATM &amp; POS</td>
<td>Individuals who send cross-border remittances</td>
<td>Fee income</td>
<td>Provides anonymous cross-border access to funds for purchases or cash</td>
<td>Various</td>
</tr>
<tr>
<td>General use cash cards</td>
<td>Debit card good at ATM &amp; POS to access pre-funded account</td>
<td>Unbanked teens and those unable to qualify for credit card</td>
<td>Fee income</td>
<td>Provides anonymous cross-border access to funds for purchases or cash</td>
<td>Various</td>
</tr>
<tr>
<td>Function-specific cards</td>
<td>Replaces paper money, tickets, and forms for a variety of functions</td>
<td>Businesses and government agencies processing high volume of cash, checks or vouchers</td>
<td>Loser cost processing</td>
<td>None apparent</td>
<td>Transit systems, Health savings accounts, Govt. benefit programs</td>
</tr>
</tbody>
</table>
Sources of Information • Resources • Contacts


Telephone interview, Kevin Bleckley, Senior Intelligence Research Specialist, Financial Crimes Enforcement Network, Jan. 22, 2014.


“7 Tips on How to Protect Yourself from Fraud” https://www.moneypak.com/ProtectYourMoney.aspx


