

## Larceny in Credit, Debit, and Electronic Transactions

Colonel James A. Young, United States Air Force (Retired)\*

In a recent article, Edward J. O'Brien and Timothy Grammel detailed the difficulty of charging military personnel under the Uniform Code of Military Justice (UCMJ) with larceny by credit card, debit card, or electronic transactions.<sup>1</sup> They note how challenging it can be to follow the money trail to determine the actual victim in such larceny cases,<sup>2</sup> and implore military prosecutors to follow the guidance provided in the *Manual for Courts-Martial (MCM)*<sup>3</sup> for charging "usual" cases.<sup>4</sup> The authors urge the Court of Appeals for the Armed Forces "to establish more clearly the parameters for what constitutes an 'unusual case.'"<sup>5</sup>

There is a better way to charge these types of offenses without having to determine the identity of the victim. Charge the accused with violating Article 134, UCMJ,<sup>6</sup> based on the federal statute proscribing the use of unauthorized access devices.<sup>7</sup>

### I. The Problem

To establish the offense of larceny,<sup>8</sup> the government must prove beyond a reasonable doubt all the elements of the offense,<sup>9</sup> including that "the property belonged to a certain person."<sup>10</sup> A problem may arise in determining who exactly owned the stolen property. The person whose name appears on the credit or debit card is often not the owner of the property stolen. Usually the victim is the merchant who accepted the credit or debit card, or the bank that issues the card and provides cash in an automated teller machine (ATM) transac-

tion.<sup>11</sup> In the past, charging the wrong victim would not necessarily have been fatal, but more recent military jurisprudence suggests otherwise.<sup>12</sup> The court-martial could save the conviction by finding the accused guilty of larceny from the proper victim by exceptions and substitutions.<sup>13</sup> But typically, the problem is not discovered until the case is on appeal, when it is too late to fix.<sup>14</sup>

The President apparently tried to resolve this issue by explaining in the 2002 Amendments to the *MCM* how to charge such offenses:

Wrongfully engaging in a credit, debit, or electronic transaction to obtain goods or money is an obtaining-type larceny by false pretense. Such use to obtain goods is *usually* a larceny of those goods from the merchant offering them. Such use to obtain money or a negotiable instrument (e.g., withdrawing cash from an automated teller or a cash advance from a bank) is *usually* a larceny of money from the entity presenting the money or a negotiable instrument.<sup>15</sup>

This provision, however, does not explain what makes a case unusual or how to charge it.<sup>16</sup>

### II. The Solution

As part of a "Joint Resolution making continuing appropriations for the fiscal year 1985, and for other purposes,"<sup>17</sup>

\* Senior Legal Advisor to the Honorable Scott W. Stucky, Associate Judge, U.S. Court of Appeals for the Armed Forces. J.D., University of Pennsylvania Law School, 1975; B.A., Lehigh University, 1968. Colonel Young served as a military judge and an appellate military judge, retiring in January 2003 as the Chief Judge of the U.S. Air Force Court of Criminal Appeals. Previous publications: *Absent Without Leave on Appeal and the Fugitive Disentitlement Doctrine*, ARMY LAW., Feb. 2015, at 3; *Court-Martial Procedure: A Proposal*, THE REPORTER, vol. 41, no. 2, 2014, at 20; *Revising the Court-Martial Selection Process*, 163 MIL. L. REV. 91 (2000); *The Accomplice in American Military Law*, 45 A.F. L. REV. 159 (1996); *Multiplicity and Lesser-Included Offenses*, 39 A.F. L. REV. 159 (1996); *The Continued Vitality of Peremptory Challenges in Courts-Martial*, ARMY LAW., Jan. 1992, at 20. The opinions expressed in this article are solely those of the author.

<sup>1</sup> Edward J. O'Brien & Timothy Grammel, *Achieving Simplicity in Charging Larcenies by Credit, Debit, and Electronic Transactions by Recognizing the President's Limitation in the Manual for Courts-Martial*, ARMY LAW., June 2015, at 5.

<sup>2</sup> *Id.* at 12.

<sup>3</sup> MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, ¶ 46.c.(1)(i)(vi) (2012) [hereinafter MCM].

<sup>4</sup> *Id.* at 12.

<sup>5</sup> O'Brien & Grammel, *supra* note 1, at 5.

<sup>6</sup> 10 U.S.C. § 934 (2012).

<sup>7</sup> 18 U.S.C. § 1029(a)(2) (2012).

<sup>8</sup> 10 U.S.C. § 921 (2012).

<sup>9</sup> *United States v. Torres*, 74 M.J. 154, 157 (C.A.A.F. 2015).

<sup>10</sup> *United States v. Cimball Sharpton*, 73 M.J. 299, 301 (C.A.A.F. 2014) (quoting MCM, *supra* note 3, pt. IV, ¶ 46.b(1)(b)).

<sup>11</sup> *See, e.g., United States v. Endsley*, No. 15-0202/AR (C.A.A.F. Jan. 14, 2015); *United States v. Gaskill*, 73 M.J. 207 (C.A.A.F. 2014) (sum. disp.); *United States v. Lubasky*, 68 M.J. 260 (C.A.A.F. 2010).

<sup>12</sup> *See United States v. Craig*, 24 C.M.R. 28, 29 (C.M.A. 1957).

<sup>13</sup> *See United States v. Marshall*, 67 M.J. 418, 421 (C.A.A.F. 2009) (holding that substituting the name of the individual from whom the accused escaped from custody was a fatal variance because it impaired the accused's ability to prepare and present a defense), *aff'd*, (C.A.A.F. Jan. 15, 2010).

<sup>14</sup> *United States v. Lubasky*, 68 M.J. 260, 265 (C.A.A.F. 2010).

<sup>15</sup> MCM, *supra* note 3, pt. IV, ¶ 46.c.(1)(i)(vi) (emphasis added); *see* MCM, *supra* note 3, A-23-17 (Analysis of the Punitive Articles).

<sup>16</sup> *See Cimball Sharpton*, 73 M.J. at 301-02 (holding that, due to the terms of the contract between the bank and the government, the Air Force, not the bank or the merchants, was the victim of the appellant's misuse of a government purchase card).

<sup>17</sup> Pub. L. No. 98-473, 98 Stat. 1837 (1984).

Congress enacted a statute proscribing the use of unauthorized credit, debit, and electronic transactions: 18 U.S.C. § 1029, entitled “Fraud and related activity in connection with access devices.”<sup>18</sup> This statute covers a wide-range of fraudulent activity with respect to credit, debit, and electronic transactions without requiring identification of the victim of a loss. Instead, the focus is on the accused’s use of a particular unauthorized access device.

Before exploring the proscriptive terms of the statute, it is important to understand the broad meaning Congress assigned to the term “access device.”

[T]he term “access device” means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, 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 paper instrument).<sup>19</sup>

This definition includes the types of access devices that are most likely to appear in a court-martial—credit, debit, and ATM cards. Most military cases should fall under subsection (a)(2):

(a) Whoever—

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating \$1,000 or more during that period;

shall if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

“[T]he term ‘unauthorized access device’ means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.”<sup>20</sup>

There is no requirement to prove there was a victim who suffered a financial loss. All that is required is proof that the accused knowingly and with intent to defraud used an unauthorized access device or devices and thereby obtained anything of value totaling at least \$1,000 in any one-year period.

“[T]he military and civilian justice systems are separate as a matter of law.”<sup>21</sup> Criminal offenses set forth in the United States Code are not applicable to military justice proceedings “except to the extent that the Code or the Manual for Courts-Martial specifically provides for incorporation of such changes.”<sup>22</sup> Article 134 specifically provides for incorporation of offenses under certain conditions:

*Though not specifically mentioned in this chapter,* [1] all disorders and neglects to the prejudice of good order and discipline in the armed forces, [2] all conduct of a nature to bring discredit upon the armed forces, and [3] crimes and offenses not capital, of which persons subject to this chapter may be guilty, shall be taken cognizance of by a general, special, or summary court-martial, according to the nature and degree of the offense, and shall be punished at the discretion of that court.<sup>23</sup>

Regardless, prosecuting an offense under Article 134 is limited by the preemption doctrine, which “prohibits application of Article 134 to conduct covered by Articles 80 through 132.”<sup>24</sup>

[W]here Congress has occupied the field of a given type of misconduct by addressing it in one of the specific punitive articles of the code, another offense may not be created and punished under Article 134, UCMJ, by simply deleting a vital element. Congress has occupied the field if it intended for one punitive article of the Code to cover the type of conduct concerned in a comprehensive . . . way.<sup>25</sup>

The preemption doctrine applies only if (1) Congress intended to limit prosecution in this area of the law to offenses defined in the UCMJ; or (2) if “the offense charged is composed of a residuum of elements of a specific offense.”<sup>26</sup>

Simply because the offense charged under Article 134, UCMJ, embraces all but one element of an offense under another article does not trigger operation of the preemption doctrine. For an offense to be excluded from Article 134 based on preemption it must be shown that Congress intended the

<sup>18</sup> Pub. L. No. 98-473, Title II, § 1602(a), 88 Stat. 2183 (1984).

<sup>19</sup> 18 U.S.C. § 1029(e)(1) (2012).

<sup>20</sup> 18 U.S.C. § 1029(e)(2) (2012).

<sup>21</sup> *United States v. McElhane*, 54 M.J. 120, 124 (C.A.A.F. 2000).

<sup>22</sup> *Id.* (quoting *United States v. Dowty*, 48 M.J. 102, 106 (C.A.A.F. 1998)).

<sup>23</sup> 10 U.S.C. § 934 (2012) (emphasis added).

<sup>24</sup> See MCM, *supra* note 3, ¶ 60.c(5)(a).

<sup>25</sup> *United States v. McGuinness*, 35 M.J. 149, 151 (C.M.A. 1992).

<sup>26</sup> *Id.* at 151–52.

other punitive article to cover a class of offenses in a complete way.<sup>27</sup>

There is no evidence that Congress intended Article 121 or any other provision of the UCMJ to cover an entire class of offenses in a complete way. Article 121 was simply intended to combine the offenses of common-law larceny, false pretense, and embezzlement.<sup>28</sup> Military appellate courts have recognized the limited reach of Article 121 by approving theft of services as an offense under Article 134, separate from larceny.<sup>29</sup>

Section 1029(a)(2), on the other hand, is in some ways broader in scope and purpose than Article 121. The purpose of Article 121 is to protect tangible property<sup>30</sup>—“any money, personal property, or article of value of any kind.”<sup>31</sup> Section 1029 covers intangible property as well—“anything of value”—and appears aimed to protect not only the property safeguarded by access devices but also the public confidence in such systems.<sup>32</sup> Therefore, the preemption doctrine does not prevent the incorporation of § 1029(a)(2) into the UCMJ under Article 134.

Military prosecutors could charge use of an unauthorized access device as a violation of clause 3 of Article 134—“crimes and offenses not capital.” But that would require proof of “every element of the crime or offense as required by the applicable law.”<sup>33</sup> Prosecutors, therefore, would have to establish that, by using the unauthorized device with the intent to defraud, the accused obtained anything of at least \$1,000 in value during a one-year period, and the accused’s conduct “affect[ed] interstate or foreign commerce.”<sup>34</sup> Additionally,

prosecution for offenses committed overseas would be restricted by the limited extraterritorial reach of the statute.<sup>35</sup>

By charging the offense under clause 1 or clause 2 of Article 134, instead of clause 3, the government could avoid having to prove that the accused obtained anything of at least \$1,000 in value in any one-year period, the accused’s conduct affected interstate or foreign commerce<sup>36</sup> or that it did not exceed the extraterritorial reach<sup>37</sup> of § 1029. “[N]either clause 1 nor clause 2 requires that a specification exactly match the elements of conduct proscribed by federal law,” as long as the elements establish an offense under one of those clauses.<sup>38</sup> Obtaining anything of value by using an unauthorized access device with the intent to defraud may, under certain circumstances, be prejudicial to good order and discipline and is certainly of a nature to bring discredit upon the armed forces.

### III. The Sticking Point—Maximum Punishment

The sticking point in charging a federal offense under Article 134 is determining the maximum punishment. By statute, the maximum sentence to confinement for a first time violation of § 1029(a)(2) is ten years.<sup>39</sup> Determining the maximum when charged under clause 1 or clause 2 of Article 134 is not as easy.

An individual convicted of violating Article 134 “shall be punished at the discretion of” the general, special, or summary court-martial hearing the case.<sup>40</sup> But that punishment “may not exceed such limits as the President may prescribe for that offense.”<sup>41</sup> The President established three general rules for

<sup>27</sup> *United States v. Erickson*, 61 M.J. 230, 233 (C.A.A.F. 2005) (quotation marks and citations omitted).

<sup>28</sup> *United States v. Willard*, 48 M.J. 147, 149 (C.A.A.F. 1998).

<sup>29</sup> *See, e.g., United States v. Firth*, 64 M.J. 508, 511 (A. Ct. Crim. App. 2006 (citing *United States v. Abeyta*, 12 M.J. 507, 508 (A.C.M.R. 1981)).

<sup>30</sup> *See United States v. Mervine*, 26 M.J. 482, 483 (C.M.A. 1988).

<sup>31</sup> UCMJ art. 121(a).

<sup>32</sup> *See, e.g., 18 U.S.C. § 1029(a)(6)(B)* (prohibiting the soliciting of another with the intent to defraud to sell information regarding an application to obtain an access device); *18 U.S.C. § 1029(a)(8)* (prohibiting the trafficking and possession of a scanning receiver).

<sup>33</sup> MCM, *supra* note 3, pt. IV, ¶ 60.b.

<sup>34</sup> *See United States v. Disney*, 62 M.J. 46, 48 (C.A.A.F. 2005).

<sup>35</sup> “A person subject to the [UCMJ] may not be punished under clause 3 of Article 134 for an offense that occurred in a place where the law in question did not apply. . . . Regardless where committed, such an act might be punishable under clauses 1 or 2 of Article 134.” MCM, *supra* note 3, pt. IV, ¶ 60.c.(4)(c)(i); *see United States v. Martinelli*, 62 M.J. 52 (C.A.A.F. 2005). The extraterritoriality provision of § 1029 provides:

Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this

section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if—

(1) the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and

(2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.

18 U.S.C. § 1029(h) (2012).

<sup>36</sup> *United States v. Leonard*, 64 M.J. 381, 383 (C.A.A.F. 2007).

<sup>37</sup> *United States v. Taylor*, 66 M.J. 293, 293 (C.A.A.F. 2008) (sum disp.) (concluding that a guilty plea to a specification alleging possession of child pornography was improvident under clause 3 because statute defining the offense to which he pled guilty did not have extraterritorial reach but affirming conviction under clauses 1 and 2).

<sup>38</sup> *Leonard*, 64 M.J. at 383 (citing *United States v. Jones*, 20 M.J. 38, 40 (C.A.A.F. 1985); *United States v. Long*, 6 C.M.R. 60 (C.M.A. 1952)).

<sup>39</sup> 18 U.S.C. § 1029(c)(1)(A)(i).

<sup>40</sup> UCMJ, art. 134, 10 U.S.C. § 934 (2012).

<sup>41</sup> UCMJ, art. 56, 10 U.S.C. § 856 (2012).

determining the maximum sentence: (1) the maximum punishment listed in Part IV of the *MCM*;<sup>42</sup> (2) for offenses not listed in Part IV but that are lesser included or closely related to those offenses, the maximum punishment is “that of the offense listed”;<sup>43</sup> and (3) for other offenses not listed in Part IV, the maximum is “as authorized by the United States Code, or as authorized by the custom of the service.”<sup>44</sup>

The offense of use of an unauthorized access device is not listed in Part IV of the *MCM*. Therefore, the question is whether (2) or (3) above applies. We start by looking at (2). Neither the President nor the Court of Appeals for the Armed Forces has defined the term “closely related.” The most straightforward approach, however, would be to compare elements. Use of an unauthorized access device appears to be closely related to the offense of larceny by wrongfully obtaining, as both share elements involving obtaining things of value by fraud. Although the statutes may serve somewhat different purposes, the elements are sufficiently similar to be closely related. Therefore, we need not analyze the offense under (3).

The President has authorized different maximum punishments for larceny based on the character of the items obtained and their value.<sup>45</sup>

(a) *Military property of a value of \$500 or less.* Bad-conduct discharge, forfeiture of all pay and allowances, and confinement for 1 year.

(b) *Property other than military property of a value of \$500 or less.* Bad-conduct discharge, forfeiture of all pay and allowances, and confinement for 6 months.

(c) *Military property of a value of more than \$500 or of any military motor vehicle, aircraft, vessel, firearm, or explosive.* Dishonorable discharge, forfeiture of all pay and allowances, and confinement for 10 years.

(d) *Property other than military property of a value of more than \$500 or any motor vehicle, aircraft, vessel, firearm, or explosive not included in subparagraph e(1)(c).* Dishonorable discharge, forfeiture of all pay and allowances, and confinement for 5 years.<sup>46</sup>

These maximum punishments should be applied to the knowing use of an unauthorized access device prosecuted under clause 1 or clause 2.

#### IV. Conclusion

Rather than trying to define the actual victim of a larceny by access device, it is better and easier to charge an accused with what he actually did: wrongfully use an unauthorized access device, under clauses 1 or 2 of Article 134.<sup>47</sup> A summary of the offense, including the maximum punishments, a model specification, the elements, and sample instructions, similar to those found in the *Military Judges’ Benchbook* for other offenses, are contained in Appendix I.

<sup>42</sup> *MCM*, *supra* note 3, R.C.M. 1003(c)(1)(A)(i).

<sup>43</sup> *Id.* R.C.M. 1003(c)(1)(B)(i).

<sup>44</sup> *Id.* R.C.M. 1003(c)(1)(B)(ii). If an offense is not included or related to an offense listed in Part IV of the *Manual for Courts-Martial*, is not an offense under the United States Code, and there is no custom of the service as to an appropriate sentence, the maximum punishment is that for a general disorder, confinement for four months. *United States v. Beaty*, 70 M.J. 39, 45 (C.A.A.F. 2011).

<sup>45</sup> *See MCM*, *supra* note 3, pt. IV, ¶ 46.e.(1).

<sup>46</sup> *Id.* ¶ 46.e.

<sup>47</sup> The Military Justice Review Group has proposed Congress enact a new provision similar, but more limited in scope, than this proposal. *See Report of the Military Justice Review Group, Part I: UCMJ Recommendations Article 121a*, at 893 (Dec. 22, 2015).

### Knowing Use of an Unauthorized Access Device

(a) Maximum Punishment:

(1) *Military property of a value of \$500 or less.* Bad-conduct discharge, forfeiture of all pay and allowances, and confinement for 1 year.

(2) *Property other than military property of a value of \$500 or less.* Bad-conduct discharge, forfeiture of all pay and allowances, and confinement for 6 months.

(3) *Military property of a value of more than \$500 or of any military motor vehicle, aircraft, vessel, firearm, or explosive.* Dishonorable discharge, forfeiture of all pay and allowances, and confinement for 10 years.

(4) *Property other than military property of a value of more than \$500 or any motor vehicle, aircraft, vessel, firearm, or explosive not included in (3) above.* Dishonorable discharge, forfeiture of all pay and allowances, and confinement for 5 years.

(b) Model Specification:

In that (rank and name of the accused) did, (location), (on or about/between) \_\_\_\_\_ 20\_\_ , with intent to defraud, knowingly use (identify the specific access device(s)) that he knew (was) (were) lost, stolen, expired, revoked, canceled, or obtained with intent to defraud, and by such use obtained (identify anything obtained) of (some value) (of a value of more than \$500), such conduct being (to the prejudice of good order and discipline in the armed forces) (of a nature to bring discredit upon the armed forces).

The specification must identify the specific access device or devices used and detail the thing(s) of value obtained. The specification should also allege any factor that will increase the maximum sentence from a bad-conduct discharge and confinement for one year—such as if the value exceeds \$500 or if the thing obtained is military property or a military motor vehicle, aircraft, vessel, firearm, or explosive.

(c) Elements:

(1) That the accused knowingly used a specific access device as alleged;

(2) That the accused did so with the intent to defraud;

(3) That the accused knew that the access device was lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

(4) That by using the access device, the accused obtained \_\_\_\_\_ of (some value); and

(5) That, under the circumstances, the accused's conduct was to the prejudice of good order and discipline or was of a nature to bring discredit upon the armed forces.

(d) Definitions and Other Instructions:

The term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, 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 paper instrument).

18 U.S.C. § 1029(e)(1) (2012).

"Intent to defraud" means an intent to obtain, through a mis-representation, anything of value and to apply it to one's own use and benefit or to the use and benefit of another, either permanently or temporarily.

*Manual for Courts-Martial, United States (MCM)* pt. IV, ¶ 49.c.(14) (2012).

"To the prejudice of good order and discipline" refers only to acts directly prejudicial to good order and discipline and not to acts which are prejudicial only in a remote or indirect sense. Almost any irregular or improper act on

the part of a member of the military service could be regarded as prejudicial in some indirect or remote sense; however, this article does not include these distant effects. It is confined to cases in which the prejudice is reasonably direct and palpable. An act in violation of a local civil law or of a foreign law may be punished if it constitutes a disorder or neglect to the prejudice of good order and discipline in the armed forces.

*MCM* pt. IV, ¶ 60.c.(2)(a).

“Discredit” means to injure the reputation of. This clause of Article 134 makes punishable conduct which has a tendency to bring the service into disrepute or which tends to lower it in public esteem.

*MCM* pt. IV, ¶ 60.c.(3).