Credit Research Foundation

Considering the legal ramifications of using Social Media in credit decisioning

Social Media: The New Reality for Credit Professionals

By Mary J. Hildebrand, CIPP/US/EU, Bruce S. Nathan and Cassandra M. Porter

This article first appeared in the 1Q 2016 edition of the CRF News. It is reprinted by permission of the Credit Research Foundation.

As John Judge, Senior Vice President at ABC Equipment Inc., casually scanned the weekly staff meeting agenda, an item caught his attention. Jane Quick, ABC's new Director of Credit, had reserved time for "Social Media." ABC provides supplies and equipment to the restaurant industry throughout the northeastern United States. What could that possibly have to do with Social Media? Curious, he called Quick for a preview.

In her new role, Quick had been investigating some disturbing trends. ABC's accounts receivable has been steadily aging. Several key customers had either closed or merged with third parties. And, perhaps most disconcerting, a few online upstarts had won business from restaurants located in ABC's sweet spot by getting access to the restaurant's management before ABC even knew about the opening. What could they know that ABC didn't?

According to Quick, ABC could improve collection of its accounts receivable and its market share by tapping into information available through social media. In fact, she intended to propose integrating social media research into ABC's credit review process from start to finish! Judge expressed reservations - after all, ABC's activities were subject to certain federal statutes, and social media was uncharted territory. Clearly, they needed more information before forging ahead.

If a similar scenario is playing out in your organization, you are not alone. Social Media offers credit professionals an unprecedented opportunity to access information regarding credit applicants outside the confines of the traditional credit application and other sources of information.

However, current laws intended to protect applicants for trade credit from unlawful practices and discrimination, still apply to the rapidly evolving area of Social Media. Increasingly, the issue confronting credit professionals is not whether to utilize information found on Social Media, but how to manage compliance and legal risks associated with that strategy.

In this initial article on how credit professionals can properly utilize Social Media, the authors explore the impact of Social Media on decisions associated with extending, limiting or terminating credit to business customers.

Setting the Stage: What Exactly is Social Media?

Commentators agree that the popular term "Social Media" encompasses a broad array of online communication platforms. In providing guidance ("Guidance") to financial institutions regarding the use of Social Media, the Federal Financial Institutions Examination Council ("FFIEC") offers an apt description:

> Social Media is a form of interactive online communication in which users can generate and share content through text, images, audio, and/or video ("Social Media"). Social Media can take many forms, including, but not limited to, (i) micro-blogging sites (e.g., Facebook, Google Plus, MySpace, and Twitter); (ii) forums, blogs, customer review web sites and bulletin boards (e.g., Yelp); (iii) photo and video sites (e.g., Flickr and YouTube); (iv) sites that enable professional networking (e.g., LinkedIn); (v) virtual worlds (e.g., Second Life); and (vi) social games (e.g., FarmVille and CityVille).[1]

Social Media is dynamic and inherently interactive, creating virtual communities for work and social activities. Individuals, organizations and businesses sponsor websites and participate on Social Media for various purposes, including interaction with current and potential customers, professional networking, or simply staying in touch with friends. Social

1 Federal Financial Institutions Examination Council (Docket No. FFIEC-2013-0002), "Social Media: Consumer Compliance Risk Management Guidance." 78 Fed. Reg. 76297-76305 (Dec. 17, 2013). Electronic mail and text messages, standing alone, are excluded from the FFIEC's definition of Social Media.

Media has the potential to provide real time data on a business applicant and their management, including, for example, today's post on Yelp, or a Facebook posting announcing the target date for opening a new location. By contrast, traditional sources of information that credit professionals use to assess creditworthiness, such as audited and unaudited financial statements, may already be stale when submitted.

Every community has rules, and Social Media is no exception. Social Media sites typically post terms of use (aka, terms of service) and a privacy policy (the "Policies") which reflect the rules applicable to profiles, content, and services available through the site. The Policies create legally binding contracts that govern the actions of Social Media providers, users and visitors to the site. Of particular interest to credit professionals, the Policies establish privacy practices governing the collection, use and disclosure of information available on the site.

Organizations and individuals that choose to share information using Social Media typically have the right to determine their audience through "privacy settings," which define the categories of users permitted access to such information. Not surprisingly, available privacy choices vary according to the applicable Policies, the preferences and consents granted by the posting party, and the status of the individual or entity seeking access to such information. For example, Facebook, the popular "micro-blogging" site, allows members to designate certain information as "public," but restrict access to more private data to individuals accepted as "friends." LinkedIn, one of the FFIEC's examples of a professional networking site, also allows members to control who may view their profile information. LinkedIn, like Facebook, considers the status of the viewer, specifically whether the viewer is a member of the LinkedIn community and the type of membership that the member has purchased from LinkedIn. Members of Facebook, LinkedIn and other Social Media sites, however, typically do not have privileges to post or modify the profiles (or "pages") of other users, particularly personal information such as name, residence, education, employment, age, or gender. In order to override existing content and post new or different profile information, the authorized user's credentials must be used (e.g., online name, password, and responses to authentication questions).

Social Media users exercise a meaningful degree of control over the content and information on their profiles and pages, and access to such materials by the public, other site members, friends and contacts. Although courts have held that there are no statutory protections for electronic information that is publicly accessible, relying on such information as a factor in extending credit may violate applicable law (see below). Moreover, the Policies also govern visitors to the Social Media site who never join or "friend" anyone. Therefore, even if a credit professional views public information on a Social Media site, use and disclosure of this information may be restricted by both applicable law and the terms in the Policies. Similarly, a Facebook wall post that is configured to be private is, by definition, not accessible to the general public.[2] Accordingly, unauthorized access and use of Social Media information designated by the users as "private," may violate the ban on fraudulent activity found in most Policies, as well as other applicable law.

Another key aspect of Social Media that credit professionals should consider is the reliability of the content and information accessed. Virtually all Social Media platform providers decline responsibility for verifying user-provided content, as reflected in their Policies. For example, the forum/customer review site Yelp permits registered users to post content and commentary regarding various businesses profiled on the site. However, the user (and not Yelp) is responsible for the reliability and veracity of that content. Yelp, like other Social Media sites, only reserves the right, although it has no obligation, to remove content that violates standards of acceptable use reflected in the Policies. Social Media sites such as Pinterest and LinkedIn, where the breadth and extent of user-created content drives the site's popularity, also provide that the user is solely liable for "user generated content" that is posted on the site.

While this allocation of responsibility for content is certainly not unique to Social Media forums, the impact of using such information in credit decisions may be significant. The issue is not that the information gleaned from Social Media is inherently unreliable. Rather, informed credit professionals should be aware that Social Media "content creators" owe no duty of loyalty or quality to anyone other than themselves. Accordingly, credit professionals should carefully consider the "weight" given to any information obtained from a Social Media site.

The Policies govern Social Media sites as a matter of contract, but legal authority for cybersecurity practices rests with the Federal Trade Commission ("FTC").[3] The FTC's enforcement responsibility includes the evaluation and enforcement of Policies that govern Social Media sites. Section 5 of the Federal Trade Commission (FTC) Act, 15 U.S.C. § 45, prohibits ''unfair or deceptive acts or practices in or affecting commerce.'' The FTC has vigorously pursued enforcement actions against Social Media sites ranging from the 2012 settlement with Facebook, Inc. (where the company agreed to submit to an independent biennial privacy audit until 2032) to the 2014 settlement with Snapchat (where the company agreed to a similar biennial 20-year audit/review period of its privacy policies).

Activities on Social Media are governed by the Policies, and through the FTC. For the most part, laws applicable to credit decisions were enacted long before Social Media became a reality. Nonetheless, these laws remain critical to the process.

Relevant Federal Laws & Regulations

There are several federal statutes that govern trade credit decision making. This article focuses on two laws integral to trade credit practices in business-to-business transactions, the Equal Credit Opportunity Act, 15 U.S.C. § 1691 et seq.

2 Recently the District Court of New Jersey reviewed this issue in the context of a wrongful termination of employment matter, Ehling v. Monmouth-Ocean Hospital Service Corp., 961 F. Supp. 2d 659, 666 (D.N.J. 2013) (citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002)).

3 The FTC authority in this area was recently affirmed by the Third Circuit in its opinion, Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015).

("ECOA") as implemented by Regulation B, and the Fair Credit Reporting Act ("FCRA"). As yet, ECOA and FCRA do not include any exceptions or special requirements applicable to Social Media, although the FFEIC has issued helpful guidance. Credit professionals pursuing a Social Media strategy to assist in their credit decisions must be mindful of the challenges inherent in applying nearly 50-year-old statutes to emerging technology. In other words, it's not a perfect fit.

Under the ECOA, it is unlawful for creditors to discriminate in any aspect of a credit transaction on the basis of an applicant's sex, marital status, race, color, religion, age, and receipt of public assistance (collectively, the "ECOA Factors"). The ECOA also requires that an applicant be notified of adverse actions, including when credit is denied, restricted or terminated. ECOA protects consumers, but is sufficiently comprehensive to implicate certain trade credit decisions. Moreover, since ECOA broadly defines "applicant" and "creditor,"[4] it applies to all credit decisions, including business credit. As a result, credit professionals are well advised to take ECOA into consideration when contemplating use of Social Media.

If a creditor, for example, treats an applicant (or a potential applicant) unfavorably based on one of the ECOA Factors, ECOA may be implicated. In particular, a creditor may not request information related to the ECOA Factors, and/or refuse to extend credit based upon one of the ECOA Factors. Commentators have gone so far as to suggest that credit professionals avoid engaging in "small talk" to avoid eliciting information covered by the ECOA Factors. Moreover, violations of ECOA do not require mal intent by the creditor; only that creditor's act(s) created a "disparate impact" on credit applicants. Under the "effects test," a creditor can violate the ECOA even when it applies the same standards to all applicants, but the standard violates the ECOA.[5] Credit professionals perusing Social Media for information regarding credit applicants may easily determine that one or more of the ECOA Factors are present. Accordingly, the potential risk of violating ECOA is increased if, and to the extent, such information is considered when making a decision about a credit applicant.

Under ECOA, if trade credit is denied, terminated or otherwise limited, the credit professional must provide a notice of the adverse action and applicant's right to request the reasons for the adverse action. The ECOA also provides that, upon applicant's timely request, the creditor must provide specific reasons for its decision to take adverse action. This requirement applies whether the information used to deny credit comes from Social Media or other sources.

The FCRA regulates the use of consumer credit reports and an individual's credit information to make credit decisions in business transactions. The FCRA applies to all written, oral, and other communications of information by a consumer-reporting agency ("CRAs") that may bear on a consumer's creditworthiness, standing or capacity, character, general reputation, personal characteristics, or mode of living. The FCRA requires that a creditor provide notice to an applicant if it is denying credit or taking any other adverse action with respect to an extension of trade credit based upon the information obtained in a consumer credit report.[6] The FCRA also requires that a creditor disclose a credit score on which the creditor relied in taking an adverse action where the credit score is based in whole or in part on information in a consumer credit report. That includes all of the key factors that adversely affected the credit score, the date the credit score was created and the name of the person or entity that provided the credit score. The FCRA also requires that a creditor seeking a credit report on a business entity's principal, who is not otherwise liable to the creditor, obtain the principal's consent. The FCRA does not apply to the use of business credit reports.[7]

In 2012, the FTC filed a suit against Spokeo, Inc., a Social Media data collector marketing profiles to human resource and recruiting departments. In its suit, the FTC alleges that Spokeo failed to adhere to the provisions of the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. ("FCRA") when collecting data and passing it on to purchasers. Spokeo and the FTC settled the action through a consent decree wherein Spokeo agreed, among other relief, to (i) pay a civil penalty of $800,000, (ii) comply with the FCRA, including providing "User Notices", (iii) submit annual "compliance reports" for the next 20 years, and (iv) maintain records necessary to demonstrate its compliance with the settlement.

For ordinary extensions of trade credit, ECOA and FCRA seem clear enough – no discrimination, adequate notice of an adverse action, disclosure and consent to access a credit report on an individual, all within statutory timeframes. In Social Media, however, the guidelines begin to blur. Suppose, for example, ABC routinely drives by restaurant locations to verify the address, the condition of the premises, or the crowds on a Saturday. Is this action materially different from checking the restaurant's Facebook page for pictures and other content to verify information provided on a credit application? Would it matter if, rather than verifying information, the credit professional intended to supplement a credit application by checking the latest Yelp reviews?

Verification would appear to be the conservative route, but strict policies are required to ensure that additional information readily available on Facebook (such as ECOA Factors) does not influence the credit decision. Yelp reviews are a gray area, not only because their veracity cannot be verified, but also due to the same unavoidable disclosure of ECOA Factors that cannot otherwise be considered. Alternatively, relying on a publicly available Facebook page

4 Under the ECOA, the term "applicant" means "any person who requests or received an extension of credit from a creditor" including a person who may become "contractually liable regarding an extension of credit." 12 C.F.R. § 1002.2(e). A "creditor" is defined under the ECOA as someone who "regularly participates in a credit decision, including setting the terms of the credit." Id. at § 1002.2(l).

5 Interagency Task Force on Fair Lending, Policy Statement on Discrimination in Lending, 59 Fed. Reg. 18,266 (Apr. 15, 1994), www.occ.treas.gov/news-issuances/federalregister/94fr9214.pdf.

6 See FTC Guidance, https://www.ftc.gov/tips-advice/business-center/guidance/using-consumer-reports-credit-decisions-what-know-about-adverse.

7 See FTC Advisory Opinion to Tatelbaum (07-26-00), www.ftc.gov/policy/advisory-opinions/advisory-opinion-tatelbaum-07-26-00.

of an existing or potential new customer or its management to learn about a possible need for the expansion of credit is likely permissible.

Information subject to restricted access on Social Media is by its nature more problematic. On Facebook and LinkedIn, members of the site may view content not available to the general public, with the next level of access reserved for friends and contacts. At each step, credit professionals must ensure that (i) they do not violate the respective Social Media sites' Policies by their access, and (ii) their use of this information does not violate applicable law (e.g., ECOA and FCRA). Although a credit professional may have sufficient privileges on a Social Media site to view data and/or information, this does not mean that the data is necessarily available to the public (and/or that prior consent is not necessary from the applicant). Therefore, while utilizing Social Media information will likely provide a credit professional with additional information, the right to use such information will remain subject to the consent of the individual or organization. Moreover, even with consent, a credit professional may not circumvent the anti-discrimination and disclosure requirements of these statutes.

Of late, certain trade creditors extending business-to-business credit are requiring access to a wider array of information that may include information related to an applicant's officers and directors, accounts with seller sites such as Amazon and e-Bay, and other sources that contribute to the so-called "Social Media Score."[8] However, given the FTC's stance on companies (like Spokeo, Inc.) that collect data similar to that of a CRA, along with ECOA's restrictions on data considered, steps to collect and utilize Social Media information should be carefully deliberated.

Recommendations: A Useful Tool, Yes, But Use of Social Media Must Be Carefully Managed

Social Media is here to stay. Its terms have become a key part of our everyday lexicon. Although considered mainstream, this does not mean that credit professionals' use of Social Media in their credit decisions without further steps, is appropriate.

In order to realize the benefits of Social Media while mitigating risk, top management must make an informed decision to permit access to Social Media and implement appropriate policies, training and oversight to ensure that applicable laws are honored.

- **Strategy**

A company's use of data gathered through Social Media must be considered by its highest levels of management. In the instance of ABC, Quick and Judge are off to an excellent start. By adding the topic to an upcoming meeting, Quick is raising these issues with management early in the process. By Judge calling Quick to discuss his concerns with the use of Social Media by Quick's department, ABC is already considering how it can best use Social Media in its decision making process. ABC should codify its policies concerning data collection and appropriate use and disclosure of such data in making credit decisions (collectively, "Social Media Policy"). Further, management should revisit the Social Media Policy on a regular basis to ensure that the policy is current and reflects recent developments.

- **Risk Management Process**

Companies should institute procedures and protocols to properly implement the Social Media Policy including, as applicable, protocols to ensure compliance with the Policies for specific Social Media sites. In the example of ABC, Quick (or another senior team member) should be charged with this responsibility and, as necessary, with authority to create a Social Media Policy team to ensure appropriate input by all stakeholders including compliance, legal, and representatives from the Board.

- **Employee Training**

Prior to implementing its Social Media Policy, company management should ensure that its personnel (employees, contractors and temporary staff) fully understand the policy and its enforcement. In our example, Quick should institute regular periodic reviews of the Social Media Policy by her department members, including disclosure practices, notice requirements, and the relative weight that should be placed on information gathered from Social Media. In this rapidly evolving environment, training should not be a one-time event. Rather, annual training should be mandatory (more frequent if applicable technology or law changes), with a process in place to address questions and issues on a real-time basis.

- **Oversight and Accountability**

The Social Media Policy should be subject to periodic review by an internal but independent company resource (e.g., the compliance department). In our example, ABC's internal review should measure the effectiveness of the Social Media Policy in addressing ABC's business concerns that led to adoption of the Social Media Policy (namely, collection issues, market share, and the paucity of current information available to the credit department compared to ABC's competitors). As determined by Quick and the reviewing parties, these results may be shared with key members of ABC's management and credit department to improve implementation and perhaps propose changes to the Social Media Policy.

- **Audit and Compliance**

In addition to more frequent internal reviews, a company's annual audit and compliance function should be updated to include the Social Media Policy. As with many other functions, companies should consider

8 See Telis Demos and Deepa Seetharaman, "Facebook Isn't So Good at Judging Your Credit After All" Wall Street Journal, Feb. 24, 2016, www.wsj.com/articles/lenders-drop-plans-to-judge-you-by-your-facebook-friends-1456309801 (timely discussion on use of social media scores).

inviting a third party consultant to evaluate the Social Media Policy in comparison to industry standards and conduct a "gap" analysis which evaluates the extent that actual practices deviate from the Social Media Policy. In the ABC example, as determined by ABC's board of directors, the audit results may be shared with ABC's management. Further, ABC's board and/or management may wish to rely on the audit results to support enterprise-wide changes to the Social Media Policy.

About the authors:

***Bruce S. Nathan**, Partner in the firm's Bankruptcy, Financial Reorganization & Creditors' Rights Department, has more than 30 years experience in the bankruptcy and insolvency field, and is a recognized national expert on trade creditor rights and the representation of trade creditors in bankruptcy and other legal matters. He has represented trade and other unsecured creditors, unsecured creditors' committees, secured creditors, and other interested parties in many of the larger Chapter 11 cases. Bruce also negotiates and prepares letters of credit, guarantees, security, consignment, bailment, tolling, and other agreements for the credit departments of institutional clients.*

***Mary Hildebrand**, CIPP/US/EU, is the founder and chair of Lowenstein Sandler's privacy and information security practice and partner in the firm's tech group. She has more than 30 years of experience in bringing technology transactions from conception to conclusion, including special expertise with respect to data privacy, security and intellectual property issues around the world.*

***Cassandra Porter** is counsel to the firm and a member of both the bankruptcy, financial reorganization & creditors' rights, and privacy and information security practice groups. She is co-chair of the New Jersey International Association of Privacy Professionals (IAPP) Knowledgenet.*

The authors wish to thank John V. Wintermute, one of the firm's associates, and Natasha Grant, one of the firm's reference librarians, for their invaluable research assistance.